ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Implementación de la Infraestructura de Comunicaciones para un Hospital previa la Implantación de un Sistema de Información Gerencial de Salud"

TESIS DE GRADO

Previa a la obtención del Titulo de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por:

Eduardo Antonio Alvarado Unamuno

Guayaquil-Ecuador

2012

AGRADECIMIENTO

A mi familia conformada por Jenny y Xavier por darme todo su apoyo, comprensión y motivación para seguir adelante con este sueño.

A mi madre y hermana por darme su apoyo, amor y fortaleza en todo momento.

DEDICATORIA

A mi Madre por su ejemplo y apoyo incondicional en todo momento.

A mi esposa e hijo.

A mis hermanos y a todos los amigos.

TRIBUNAL DE GRADUACIÓN

Ing. Lenin Freire Cobo

DIRECTOR MSIG

Ing. Albert Espinal

DIRECTOR DE TESIS

Ing. Karina Astudillo

MIEMBRO TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente; y el patrimonio intelectual de la misma a la **ESCUELA SUPERIOR POLITECNICA DE LITORAL"**

(Reglamento de Graduación de la ESPOL)

Eduardo A. Alvarado Unamuno

RESUMEN

En el contexto histórico, social y cultural, en el que nuestra sociedad se desarrolla, resulta ineludible considerar la informática y el internet como factor propulsor de un cambio en la manera con que se brindan los servicios de salud. Avances en los medios y procedimientos de comunicación y el desarrollo tecnológico de avanzada, son aspectos que deben ser considerados con otros de índole político-social, entre los que se pueden mencionar el desarrollo del país, la disponibilidad económica, el nivel cultural, servicios de salud y las políticas de Estado.

En este contexto las TIC deben considerarse parte de los instrumentos que permiten mejorar los servicios de salud, logrando brindar servicios que anteriormente solo se concentraban en los hospitales de las grandes ciudades. En la introducción de tecnologías de sistemas de computación en la salud, se hace necesario eliminar los obstáculos debido a una obstinada resistencia ante el cambio; a la falta de información y a la desconfianza. La difusión de la cultura informática representa un gran desafío para toda la estructura en el área de salud y se extiende a otras estructuras del mundo del trabajo y de la sociedad.

El propósito de este trabajo de Tesis es el rediseño de la infraestructura de comunicaciones de un Hospital previa la implantación de un sistema de información

gerencial de salud, permitiendo al hospital mejorar los servicios de salud que brinda a sus pacientes.

Este trabajo consta de seis capítulos. El CAPITULO 1, CONSIDERACIONES GENERALES DE LA RED DEL HOSPITAL, se contextualiza, describe lo observable de la red actual del hospital y sus consecuencias en los servicios brindados a los pacientes; se culmina con la solución propuesta.

El CAPITULO 2, abarcan los FUNDAMENTOS TEÓRICOS, se describen los procesos investigativos de la realización del presente trabajo: Los fundamentos técnicos utilizados para lograr los resultados de manera adecuada.

El CAPITULO 3, hace relación a la VALORACIÓN DE LOS DISPOSITIVOS DE RED Y ANÁLISIS DE RIESGOS, en donde se describen las variables que intervienen en el problema. Los dispositivos activos de la red, acciones de contingencia ante fallos de los mismos, análisis de riegos y el análisis de costo/beneficio de la implementación de una nueva red como una forma de ayuda a mejorar los servicios de salud brindados por el hospital.

EL CAPITULO 4, abarcan LOS SERVICIOS PROPUESTOS PARA LA RED LAN Y WAN, se describen los procesos del rediseño de la red para logra una red escalable y con alta disponibilidad, también los procedimientos técnicos utilizados.

EL CAPITULO 5, corresponde a las PRUEBAS DE DESEMPEÑO DE LA NUEVA RED, se realizan las pruebas respectivas para comprobar las caracteristicas de alta disponibilidad de la nueva implementación de la red

EL CAPITULO 6, donde se plasma las Conclusiones y Recomendaciones pertinentes productos de este trabajo de investigación.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

INDICE DE GRÁFICOS

INTRODUCCIÓN

El desarrollo de tecnologías que facilitan significativamente el procesamiento de la información y colaboran a su obtención, que se materializan en ordenadores cada vez más eficientes y sistemas de comunicaciones más sofisticados, eficientes y seguros, han generado una profunda revolución socio-cultural y nuevos esquemas científicos, económicos y financieros.

"Las evidencias han demostrado que a pesar de la gran cantidad de acciones, descubrimientos y desarrollos tecnológicos en el área de la medicina, la expectativa de vida se ha incrementado fundamentalmente merced al desarrollo socioeconómico y cultural de los pueblos"[1]. No obstante, las relaciones de costo han sido francamente altas y continúan creciendo en función directa con la tecnología. Los gobiernos se plantean nuevas alternativas para mejorar estos paradigmas que ha dejado a la medicina como altamente ineficiente en la relación costo-beneficio.

El trabajo del médico es el de atender las necesidades de los pacientes utilizando el conocimiento acumulado por la medicina durante más de 5000 años y, sobre todo, en el último siglo. "Se dice que los médicos utilizan unos dos millones de piezas de información en el cuidado de los pacientes, que un tercio del tiempo lo pasan registrando y sintetizando información y que un tercio de los costos de un hospital

[1] Fuente: Libro de Medicina: **VIEJOS Y NUEVOS CONCEPTOS EN MEDICINA Y SALUD (Dr Mareco, Dr Rinesi, Dr Ramos) Facultad de Medicina UNNE**

tiene que ver con la comunicación personal y profesional"[2]. Hoy más que nunca resulta claro que el médico no puede desempeñarse sólo con la información que ha acumulado en su memoria.

Como un lógico proceso de desarrollo, la medicina ha ido asimilando la introducción de las computadoras para agilizar y mejorar los procesos de apoyo médico, teniendo una gran influencia, la que sigue aumentando más cada día con la introducción de la Inteligencia Artificial en la vigilancia del paciente con complejos equipos biomédicos, realización de procesamiento voluminoso de información para la toma de decisiones y muchas otras aplicaciones. Podemos hablar entonces del surgimiento de la Informática Médica, que comprende una amplia gama de cuestiones de la organización y del uso de la información biomédica. El objetivo de la Informática Médica es reforzar y mejorar la toma de decisiones médicas y la atención al paciente.

Por más de una década las iniciativas relacionadas a la salud-*e* en Ecuador se desarrollaron de manera aislada unas de otras. En el año 2001, con motivo de la convocatoria y trabajo de la Agenda Nacional de Conectividad (ANC), se logró generar una línea de base sobre los intereses y progresos de las instituciones y personas que trabajaban en el tema.

---

[2] Fuente: Libro de Medicina: **VIEJOS Y NUEVOS CONCEPTOS EN MEDICINA Y SALUD (Dr Mareco, Dr Rinesi, Dr Ramos) Facultad de Medicina UNNE**

Con la iniciativa de la ANC muchos actores comenzaron a vincularse. El Gobierno asumió una participación activa y la comunidad de profesionales médicos, informáticos en salud, biomédicos y usuarios en general, empezaron a informarse sobre las ventajas y usos de la salud-e.

La Agenda definió cinco temas relevantes para el desarrollo del país, uno de los cuales fue la telemedicina. Para cada tema se presentó un diagnóstico y se establecieron objetivos, metas, estrategias y un plan de acción a corto y mediano plazo. Entre los objetivos para la telemedicina en Ecuador destaca el "enlazar y ofrecer una comunicación interactiva entre las unidades médicas distantes con centros en ciudades principales, a través de una Red Nacional de Telesalud".

Otra iniciativa de importancia en Ecuador ha sido la creación en 2005 de FUNDETEL, una ONG sin fines de lucro conformada por un grupo de médicos y profesionales de la salud. Es una institución abierta que busca integrar organizaciones y personas con voluntad de hacer y aportar con recursos humanos, económicos y tiempo, que tiene entre sus propósitos fomentar y difundir el uso y beneficios de la telemedicina y salud-e, así como crear una red que comparta información, conocimientos y experticias para la optimización de recursos.

Dado esto, resulta obvio pensar que se depende de las redes, sin embargo sobre todo si no hay un sistema alterno, puede propiciar que toda la organización se paralice

cuando la red se descompone, y, por otro lado, se requiere de un mantenimiento de la red para vencer la obsolescencia. Esta dependencia puede implicar que el médico se paralice cuando no tiene acceso a la información de los pacientes, por ejemplo por reparaciones o mantenimiento preventivo, y que tienda a utilizarse en casos en los que no sería estrictamente necesario, causando una saturación de los servicios y una riesgosa espera para los pacientes en los que es indispensable.

La presente tesis tiene como uno de sus objetivos específicos rediseñar la red de un Hospital que forma parte de una red de Hospitales para garantizar una red médica con alta disponibilidad y escalable para evitar fallas en sistema y así perder el acceso a una información que puede ser esencial para atender debidamente al paciente.

OBJETIVO

El presente trabajo de tesis tiene por objetivo ayudar a optimizar la infraestructura de red para mejorar los servicios de salud que brinda el hospital para lo cual se presentan los siguientes objetivos generales y específicos.

Objetivo General de la Tesis

- Implementar una red de comunicaciones que posea alta disponibilidad y escalabilidad para un hospital, previa la implantación de un sistema de información gerencial de salud.

Objetivos Específicos de la Tesis

- Definir los requerimientos actuales y futuros de las comunicaciones del hospital.
- Realizar un análisis de costo y beneficio de la solución.
- Diseñar la arquitectura de comunicaciones.
- Definir el sistema de monitoreo y gestión de los dispositivos de comunicaciones.
- Realizar la simulación de la nueva red de comunicaciones.
- Implementación de la red de comunicaciones.

CAPÍTULO 1

CONSIDERACIONES GENERALES DE LA RED DEL HOSPITAL

1.1 Antecedentes

La tecnología de la computación ha tenido una gran influencia en la Medicina y ésta sigue aumentando cada vez más. Algunos de los usos de las computadoras en este campo son las pruebas para detectar e identificar alteraciones, como por ejemplo, la tomografía axial computarizada, los análisis de electrocardiogramas por computadora, los monitores de procesos fisiológicos, la automatización de las líneas en laboratorios clínicos, el control de los resultados entrega de medicamentos, y otros. Los profesionales de la salud utilizan también las computadoras para controlar y planificar sus servicios.

La automatización y la informatización de las líneas de proceso en el laboratorio y pruebas de gabinete hacen que los datos transferidos a la computadora sean procesados en forma muy rápida y sean capaces de ser comparados con pruebas y valores estándar establecidos en el programa de cómputo. En pocos minutos, los resultados de la prueba son reportados y si estuvieran fuera de los límites fijados, el

programa podría sugerir los procedimientos que deben repetirse o las pruebas adicionales que deban realizarse. Es posible que la computadora esté ejecutando en este caso, un programa de sistema experto, con el objeto de sugerir posibles diagnósticos y explicar resultados anormales de las pruebas. Sin embargo, dado la creciente necesidad de implementar hardware y software en aplicaciones médicas hacen que las redes de computadoras deban soportar aplicaciones de software cada vez más demandantes de ancho de banda.

Cuando se implementan redes de computadoras en hospitales o centros de salud las mismas deben de tener una alta disponibilidad, ya que se vuelven críticas dada la dependencia de los sistemas informáticos hospitalarios del buen funcionamiento de la red.

1.2 Descripción del Problema

Dado que la gran mayoría de los equipos de medicina actualmente pueden ser conectados a redes de computadores y de esta manera se pueden obtener resultados que pueden ser almacenados en formato digital y estén disponibles por cualquier especialista médico a través de un sistema informático que asocie todos estos resultados a su historia clínica. Con estos requerimientos de información que debe estar actualizada y disponible en cualquier momento, las redes de computadoras en ambientes hospitalarias requieren tener una alta disponibilidad y confiabilidad.

Por lo tanto estas redes requieren diseños escalables que permitan a los administradores de red adaptarse rápidamente a nuevos requerimientos que los ambientes de salud requieren, por lo tanto a continuación se detallan los problemas más comunes en esta red.

1.- No existe comunicación entre los equipos médicos y las redes de comunicación del hospital.

2.- La información de rayos X, resultados de exámenes de sangre, etc. se manejan a través de placas o en sistemas independientes y no están integrados en una historia clínica, el paciente todavía tiene que llevar sus resultados.

3.- Redes de comunicaciones no apropiadas para Teleconsultas, Telemonitoreo etc., ya que carecen de infraestructura adecuada.

4.- Infraestructura de comunicaciones sin contingencia, para mitigación ante fallas.

5.- Infraestructura de comunicaciones no apta para transportar imágenes de alta definición (rayos x, tomografías, etc.) en forma rápida.

6.- Pérdida de información al no tener un sistema de información que integre todas las fuentes de datos.

1.3 Infraestructura de la Red LAN y WAN Actual del Hospital.

La infraestructura actual del hospital presenta una topología física estrella, los equipos que la componen son un Cisco 4507R cumpliendo las funciones de conmutador de núcleo y agregación, mientras que como conmutador de acceso están los Cisco 2960.

A continuación se adjunta el Gráfico de la red LAN actual del hospital.

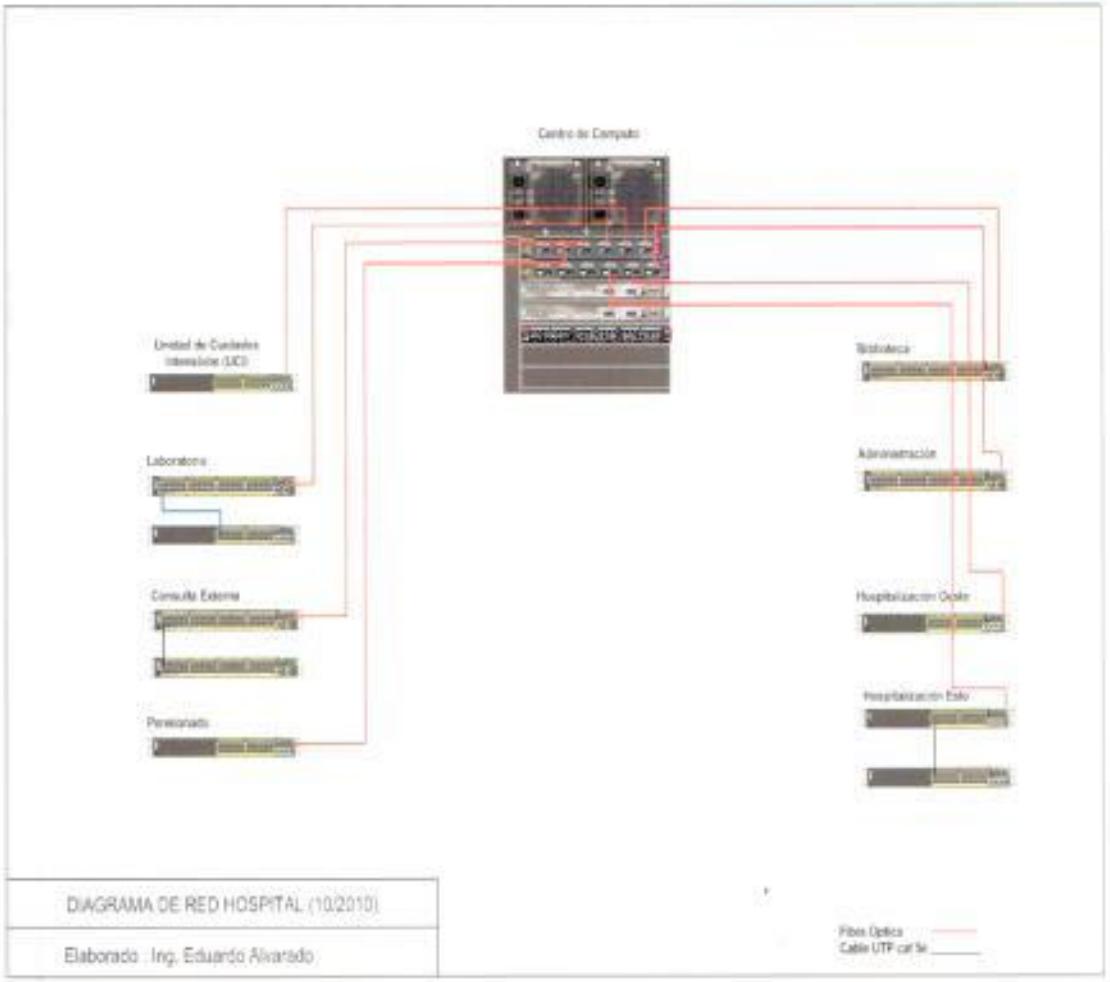


Gráfico N° 1 : Diagrama de Red LAN del Hospital
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

Cuadro N° 1
Inventario de Equipos Activos LAN

INVENTARIOS EQUIPOS LAN DEL HOSPITAL		
UBICACION	DESCRIPCIÓN	
	MARCA	MODELO
ADMINISTRACIÓN	CISCO	Catalyst WS-C2960-48TC - L V03
BIBLIOTECA	CISCO	Catalyst WS-C2960-48TC - L V03
CONSULTA EXTERNA	CISCO	Catalyst WS-C2960-48TC - L V03
CONSULTA EXTERNA	CISCO	Catalyst WS-C2960-48TC - L V03
CONTROL PRINCIPAL	CISCO	Catalys WS-C4507R
CONTROL PRINCIPAL	CISCO	Catalyst WS-C2960G-48TC - L V02
CONTROL PRINCIPAL	CISCO	Catalyst WS-C2960-24TC - L V03
HOSPITALIZACIÓN - ALA OESTE	CISCO	Catalyst WS-C2960-24TC - L V03
HOSPITALIZACIÓN – ALA ESTE	3COM	3C16471
HOSPITALIZACIÓN – ALA ESTE	CISCO	Catalyst WS-C2960-24TC - L V03
HOSPITALIZACIÓN (UCI)	CISCO	Catalyst WS-C2960-24TC - L V03
LABORATORIO	CISCO	Catalyst WS-C2960-48TC - L V03
LABORATORIO	CISCO	Catalyst WS-C2960-24TC - L V03
PENSIONADO	CISCO	Catalyst WS-C2960-48TC - L V03

Fuente : Datos de la Investigación Hospital.
Elaboración: Eduardo Alvarado Unamuno

Cuadro N° 2
Inventario de Equipos Activos WAN

INVENTARIOS EQUIPOS WAN DEL HOSPITAL		
UBICACION	DESCRIPCIÓN	
	MARCA	MODELO
Hospital 1	CISCO	Enrutador 806
Hospital 2	CISCO	Enrutador 831
Hospital 3	CISCO	Enrutador 831
Hospital 4	CISCO	Enrutador 831
Hospital 5	CISCO	Enrutador 2801
Hospital 6	CISCO	Enrutador 831
Central	CISCO	Enrutador 2801
Oficinas	CISCO	Enrutador 831
Fundaciones	CISCO	Enrutador 831
Comisariato	CISCO	Enrutador 831
Bodega	CISCO	Enrutador 1941

Fuente : Datos de la Investigación Hospital.
Elaboración: Eduardo Alvarado Unamuno

A continuación presentamos el diagrama de alto nivel de la red WAN.

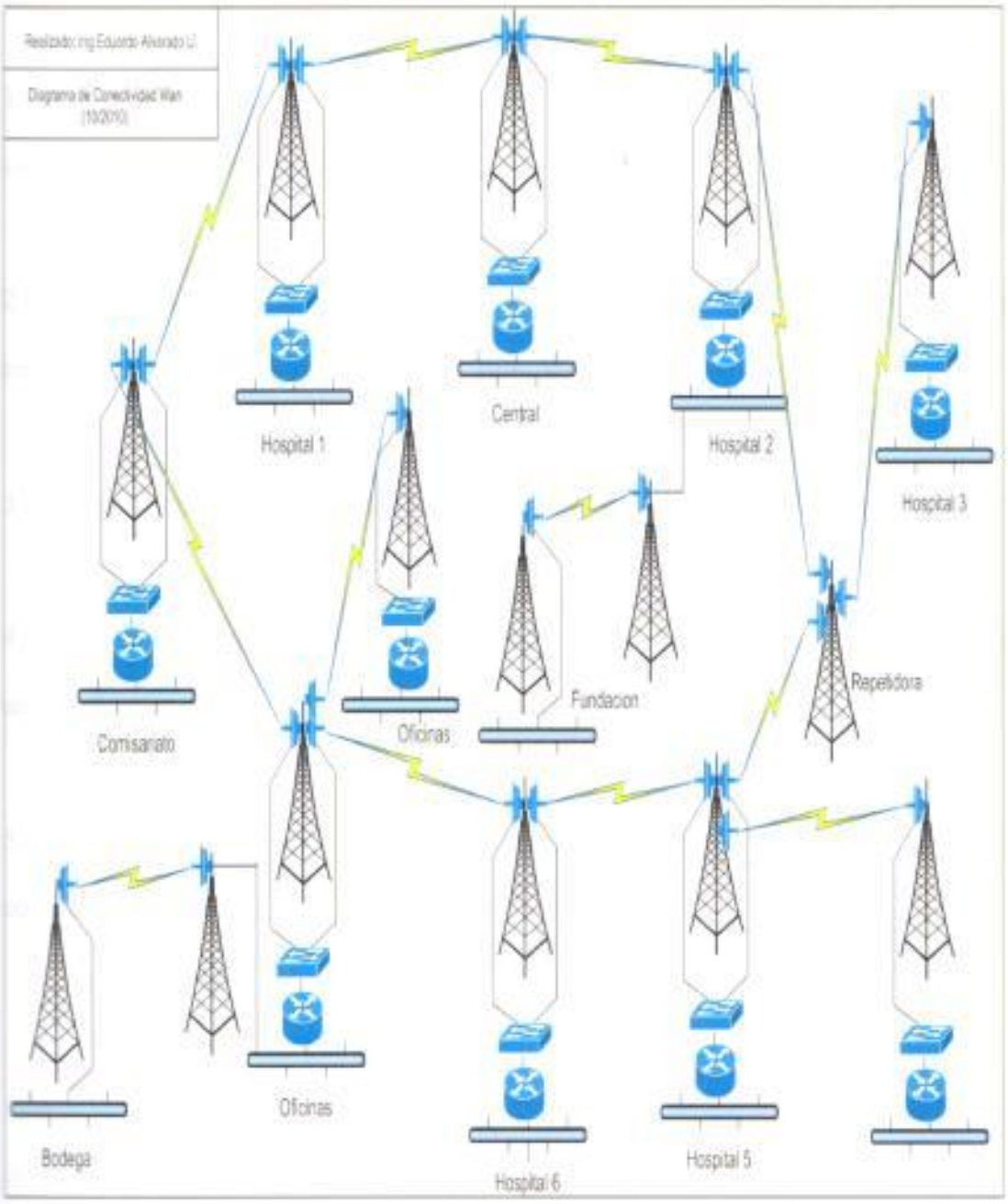


Gráfico N°2 : Diagrama de Red WAN del Hospital
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

1.4 Solución Propuesta

La solución es la instalación de una infraestructura de comunicaciones que permita:

1.- Implementar un esquema de comunicaciones que sea escalable y establezca esquemas de alta disponibilidad.

2.- El desarrollo e implantación de nuevas tecnologías que requiere la medicina actual en nuestro país como la Telemedicina y Teleconsulta.

3.- La implantación del nuevo sistema de información adquirido por el hospital.

4.- Transportar e integrar imágenes en formato digital dadas por los equipos médicos en las historias clínicas.

5.- La implementación de un sistema de monitoreo y gestión de la infraestructura de comunicaciones.

CAPITULO 2

FUNDAMENTOS TEÓRICOS.

2.1 Modelo de Capas

El diseño de la nueva arquitectura de red será basada en una arquitectura de red de capas el cual utiliza un modelo de red jerárquica. Históricamente utilizada en el diseño de redes LAN y WAN en empresas.

Gráfico N°3 : Modelo Jerárquico en Capas
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

El modelo de red jerárquica ofrece una visión modular de una red, por lo que es más fácil para diseñar y construir una infraestructura escalable. La estructura de red jerárquica está compuesta por el acceso, la distribución y el núcleo. Cada capa tiene su propia función, que se utilizan para desarrollar un diseño jerárquico.

El modelo jerárquico proporciona un marco modular que permite flexibilidad en el diseño y facilita la implementación y la solución de problemas. El modelo de red jerárquica se divide en capas las cuales son acceso, distribución, y núcleo, las cuales tienen las siguientes características.

Capa de Acceso: Se utiliza para permitir el acceso de usuarios a los dispositivos de red. En una red tipo campus, en general la capa de acceso, incorpora los dispositivos de conmutación LAN con puertos que proporcionan conectividad a las estaciones de trabajo, teléfonos IP, servidores, y puntos de acceso inalámbrico. En el entorno de la WAN, la capa de acceso a los tele trabajadores o los sitios remotos puede proporcionar la entrada a la red corporativa a través de la tecnología WAN.

Capa de distribución: Agrega los armarios de cableado, utilizando conmutadores para segmentar grupos de trabajo y aislar problemas de red en un entorno de campus. Del mismo modo, se agrega tráfico de conexiones WAN en el borde del campus y proporciona una conectividad basada en políticas.

Capa de núcleo: Diseñado para conmutar paquetes tan rápido como sea posible. Dado que el núcleo es fundamental para la conectividad, se debe proporcionar un alto nivel de disponibilidad y que se adaptan rápidamente a los cambios. También se proporciona la escalabilidad y la rápida convergencia y el punto de entrada a la red de los dispositivos finales.

2.1.1 Capa de Acceso.

La capa de acceso agrega a los usuarios finales y ofrece los enlaces ascendentes para la conexión a la capa de distribución. La capa de acceso puede soportar múltiples funciones las cuales mencionamos a continuación:

Alta disponibilidad: En la capa de acceso, la alta disponibilidad está soportada a través de atributos o funcionalidades del hardware y software. Con el hardware, a nivel de sistema redundancia se puede realizar utilizando módulos supervisores redundantes y fuentes de alimentación. También puede ser proporcionado por la redundancia en la puerta de enlace predeterminada, con doble conexiones desde los conmutadores de acceso a los conmutadores de capa de distribución. Con software la alta disponibilidad está soportada mediante el uso del protocolo de Enrutador de Primer salto (FHRP), el Protocolo de Enrutador Activo Espera (HSRP), el Protocolo de Redundancia de Enrutador Virtual (VRRP) y el Protocolo de Balanceo de Carga de Puerta de Salida (GLBP).

Convergencia: La capa de acceso soporta Alimentación a través de Ethernet (PoE) para la telefonía IP y puntos de acceso inalámbricos, permitiendo a los clientes converger en sus redes voz y datos proporcionando acceso itinerante para los usuarios de la red inalámbrica.

Seguridad: La capa de acceso proporciona servicios de seguridad contra acceso no autorizado a la red mediante el uso de herramientas tales como el estándar IEEE 802.1x, seguridad de puertos, espionaje DHCP, inspección Dinámica ARP (DAI) y guardia de la fuente IP.

Calidad de servicio (QoS): La capa de acceso permite la priorización de tráfico de misión crítica utilizando la clasificación del tráfico y las colas tan cerca de la entrada de la red como sea posible. La cual es compatible con el uso de límite de confianza QoS.

Multidifusión IP: La capa de acceso soporta eficientemente en las redes la administración del ancho de banda con características como el Protocolo de Administración de Grupo de Internet (IGMP).

2.1.2 Capa de Distribución.

La capa de agregación y distribución de tráfico de todos los nodos y enlaces ascendentes desde la capa de acceso, proporciona conectividad basada en políticas, como se ilustra en el Gráfico 5, también proporciona alta disponibilidad y calidad de servicio estas son las características mas importantes de esta capa.

La alta disponibilidad se proporciona normalmente a través de caminos dobles de la

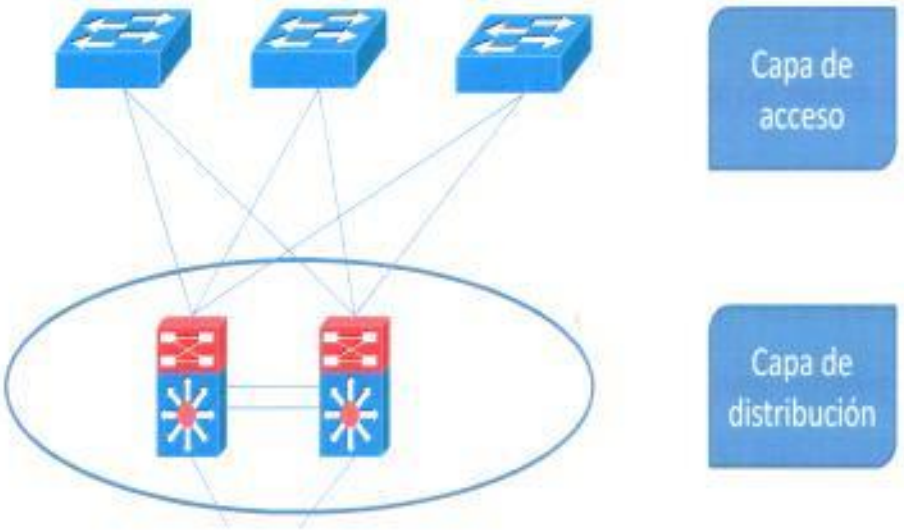


Gráfico N°4 : Capa de Distribución
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

Capa de distribución hasta el núcleo y de la capa de acceso a la capa de distribución. El Balanceo de carga en capa 3 permite que ambos enlaces ascendentes de la distribución hacia la capa del núcleo puedan ser utilizados.

La capa de distribución es el lugar donde el enrutamiento y la manipulación de paquetes se llevan a cabo y puede ser un límite de enrutamiento entre el acceso y el núcleo. La capa de distribución representa un punto de redistribución entre los dominios de enrutamiento o la demarcación entre protocolos de enrutamiento estático y dinámico. La capa de distribución realiza tareas tales como control de enrutamiento y filtrado para implementar la conectividad basada en políticas y QoS. Para mejorar aún más el rendimiento del protocolo de enrutamiento, la capa de distribución sumariza las rutas desde la capa de acceso. En algunas redes, la capa de distribución

ofrece una ruta por defecto a la capa de acceso y en él se ejecutan protocolos de enrutamiento dinámico cuando se comunica con los enrutadores del núcleo.

La capa de distribución utiliza una combinación de capa 2 y conmutación multicapa para segmentar grupos de trabajo y aislar problemas de red, evitando que afecten la capa del núcleo. La capa de distribución puede ser utilizada para terminar las redes virtuales de los conmutadores de la capa de acceso. La capa de distribución conecta servicios de red a la capa de acceso y se implementa QoS, seguridad, balanceo de carga y las políticas de enrutamiento. La capa de distribución proporciona redundancia de puerta de enlace predeterminada mediante un FHRP, como HSRP, GLBP o VRRP, para permitir la falla o la eliminación de uno de los nodos de distribución, sin afectar la conectividad de los nodos finales con la puerta de enlace predeterminada.

2.1.3 Capa de Núcleo.

La capa de Núcleo proporciona escalabilidad, alta disponibilidad y rápida convergencia a la red, como se ilustra en el Gráfico N° 6. La capa del Núcleo es la columna vertebral para la conectividad del campus, y es el punto de partida para la agregación de las otras capas y módulos en la arquitectura de capas. El núcleo proporciona un alto nivel de redundancia y puede adaptarse a los cambios rápidamente. Dispositivos centrales son más fiables cuando se puede acomodar fallas

por desvío de tráfico y pueden responder rápidamente a los cambios en la topología de la red.

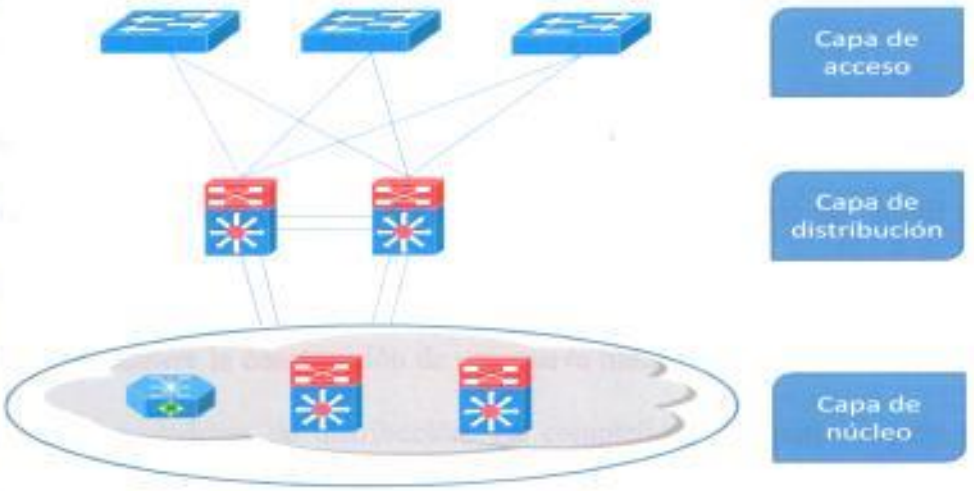


Gráfico N°5 : Capa de Núcleo
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

Los dispositivos de núcleo escalables permiten implementar protocolos y tecnologías, rutas alternativas y balanceo de carga. La capa de núcleo ayuda en la escalabilidad durante el crecimiento futuro.

El núcleo es alta velocidad, generalmente conmutadores de nivel 3 usan servicios de aceleradores de hardware. Para la convergencia rápida en torno a una falla en el enlace o nodo, el núcleo utiliza interconexiones redundantes punto a punto de capa 3 porque este diseño produce el más rápido y más resultados deterministas de convergencia. La capa del núcleo está diseñado para evitar cualquier manipulación de paquetes, como la comprobación de las listas de acceso y filtrado, lo que haría más

lento el conmutación de paquetes. No todas las implementaciones del campus requieren una capa de núcleo. El núcleo y la capa de distribución funciones se pueden combinar en la capa de distribución de un campus pequeño.

Sin una capa de núcleo, los conmutadores de la capa de distribución deben ser totalmente mallada, como ilustra el Gráfico 6. Este diseño puede ser difícil de ser escalable, y aumenta los requisitos de cableado, ya que cada conmutador de distribución requiere la construcción de una nueva malla completa de conectividad a todos los conmutadores de distribución. La complejidad del enrutamiento en un diseño de malla completa se incrementa a medida los nuevos vecinos se suman.

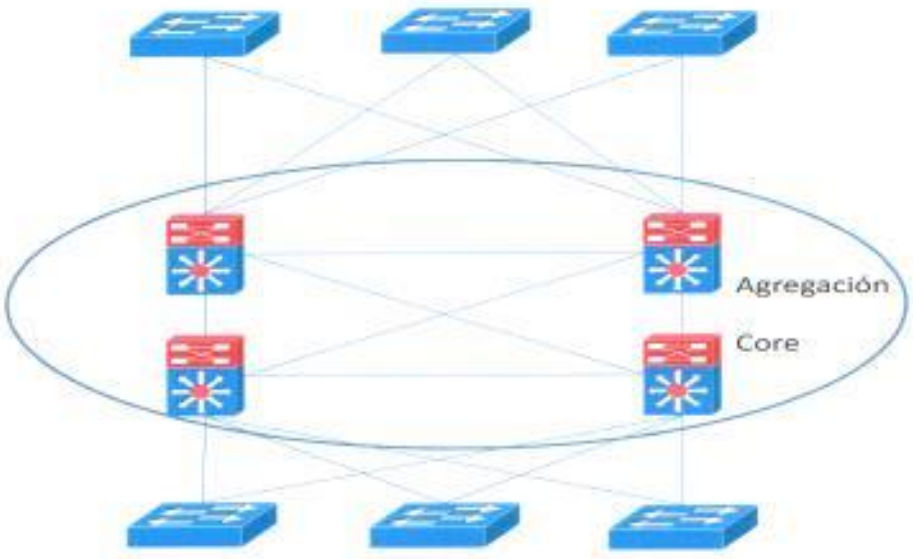


Gráfico N°6 : Red Mallada
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

2.2 Consideraciones de Diseño en Conmutadores.

2.2.1 Guías de Diseños Óptimos en Conmutadores.

Las arquitecturas de capa 2 se basan en las siguientes tecnologías para crear una topología determinística de alta disponibilidad: Protocolo de Árbol Expandido (STP), Troncales (ISL/802.1q), Detección de enlace unidireccional (UDLD), y Ether Canal.

En las siguientes secciones veremos los modelos de diseño y prácticas recomendadas para alta disponibilidad y convergencia óptima en capa 2.

2.2.2 Prácticas Recomendadas para la Configuración de Árbol Expandido.

Para las topologías de red más determinista y de alta disponibilidad, los requerimientos para soportar el protocolo de árbol expandido deben ser evitados por el diseño. Pero puede ser que se tenga que poner en práctica STP por varias razones:

1.- Cuando una Red Virtual (VLAN) abarca varios conmutadores en la capa de acceso para soportar aplicaciones del negocio.

2.- Para evitar bucles de lado del usuario, incluso si en el diseño se recomienda, no dependerá de STP resolver fallas de enlace o eventos en falla de nodos, el STP es necesario para proteger contra los bucles del lado de usuario. Hay muchas maneras en

que un bucle se puede introducir en el lado del usuario en los puertos de la capa de acceso. Errores de cableado, estaciones finales mal configuradas, o usuarios malintencionados pueden crear un bucle. STP es necesario para garantizar una topología libre de bucles y para proteger al resto de la red de problemas creados en la capa de acceso.

En ciertas ocasiones seguridad se recomienda deshabilitar STP en la capa de acceso, en la práctica no es recomendable porque el riesgo de pérdida de conectividad sin STP es mucho mayor que cualquier información que por STP pueda ser revelada.

Si es necesario implementar STP, use el protocolo Árbol Expandido Rápido por Red Virtual mas (RPVST +). También se puede tomar ventaja de las mejoras de STP utilizando el juego de funcionalidades de STP.

2.2.3 Funcionalidades del Protocolo de Árbol Expandido.

Las mejoras para STP son las siguientes. Se debe tener en cuenta que las mejoras marcados con un * son también compatibles con el protocolo de Árbol Expandido Rápido por Red Virtual mas [RPVST +].

- Puerto Rápido *: Causas que una interfaz LAN de Capa 2 configurada como un puerto de acceso entre en el estado de envío de inmediato, sin pasar por los

estados de escucha y aprendizaje. Use puerto rápido sólo cuando se conecta una sola estación a un puerto de acceso de capa 2.

- Enlace Ascendente Rápido: Ofrece una convergencia de tres-cinco segundos después que un enlace falla y logra balancear la carga entre los enlaces redundantes de capa 2 con grupos enlaces ascendentes.

- Troncal Rápido: Corta el tiempo de convergencia dado por el comando "max_age" provocado por una falla indirecta. Troncal Rápido se inicia cuando un puerto raíz o puerto bloqueado en un dispositivo de red recibe un paquete del Protocolo de Unidad de Datos de Puente (BPDU) inferior desde su puente designado.

- Bucle de guardia*: Evita que un puerto alternativo o la raíz de convertirse en el designado en ausencia de paquetes del Protocolo de Unidad de Datos de Puente (BPDU). Bucle de guardia ayuda a evitar bucles de puenteo que podrían ocurrir debido a una falla en el enlace unidireccional en un enlace punto a punto.

- Raíz de guardia: Asegura la elección del conmutador raíz en un conmutador específico mediante la prevención de que conmutadores externos no se conviertan en el conmutador raíz.

- Guardia de Protocolo de Unidad de Datos de Puente*: Cuando se configura en un puerto que tiene habilitado Puerto Rápido, la funcionalidad de Guardia de Protocolo de Unidad de Datos de Puente inhabilita al puerto que recibe un de Protocolo de Unidad de Datos de Puente.

- Detección de enlace unidireccional (UDLD): Controla la configuración física de conexiones de fibra óptica y cobre y detecta cuando conexiones de una sola vía existen. Cuando un link unidireccional se detecta, la interfaz se inhabilita y el sistema se alerta.

2.2.4 Protocolo de Árbol Expandido Estándar.

El Protocolo de Árbol Expandido habilita a la red para bloquear de forma determinista interfaces y proporcionan una topología de red libre de bucle en una red con enlaces redundantes. Existen varias variedades del Protocolo de Árbol Expandido:

El Protocolo de Árbol Expandido (STP) es la versión original IEEE 802.1D (802.1D-1998), que proporciona una topología libre de bucles en una red con enlaces redundantes.

Árbol Expandido Común (CST) supone una instancia del Protocolo de Árbol Expandido para toda la red de puentes, sin importar el número de redes virtuales.

Protocolo de Árbol Expandido por Red Virtual mas (PVST +) es una mejora del fabricante Cisco del protocolo de árbol expandido, que proporciona una instancia por separado de 802.1D para cada red virtual configurada en la red. La instancia independiente soporta Puerto Rápido, Enlace de Subida Rápido, Troncal Rápida, Guardia Protocolo de Unidad de Datos de Puente, Filtro de Lazo de Guardia Protocolo de Unidad de Datos de Puente, y Lazo de Guardia.

La versión *802.1D-2004* es una versión actualizada de la norma de STP.

Árbol Expandido Múltiple (MST) es un estándar IEEE inspirada en el antiguo protocolo propietario de Cisco Multi Instancias del Protocolo de Árbol Expandido (MISTP). MST mapea múltiples redes virtuales en la misma instancia de Árbol Expandido. La implementación de Cisco de MSTP es MST, que proporciona hasta 16 instancias del Protocolo Rápido de Árbol Expandido (RSTP, 802.1w) y combina muchas redes virtuales con la misma topología física y lógica en una instancia común de RSTP. Cada instancia soporta Puerto Rápido, Enlace de Subida Rápido, Troncal Rápida, Guardia Protocolo de Unidad de Datos de Puente, Filtro de Lazo de Guardia Protocolo de Unidad de Datos de Puente, y Lazo de Guardia.

RSTP, o IEEE 802.1w, es una evolución del STP que proporciona una convergencia más rápida que STP.

Protocolo Rápido de Árbol Expandido por Red Virtual mas (RPVST +) es una mejora de Cisco de RSTP que usa PVST+. El proporciona una instancia independiente de 802.1w por red virtual. La instancia independiente soporta Puerto Rápido, Enlace de Subida Rápido, Troncal Rápida, Guardia Protocolo de Unidad de Datos de Puente, Filtro de Lazo de Guardia Protocolo de Unidad de Datos de Puente, y Lazo de Guardia.

El Gráfico 7 ilustra las ubicaciones recomendadas para STP:

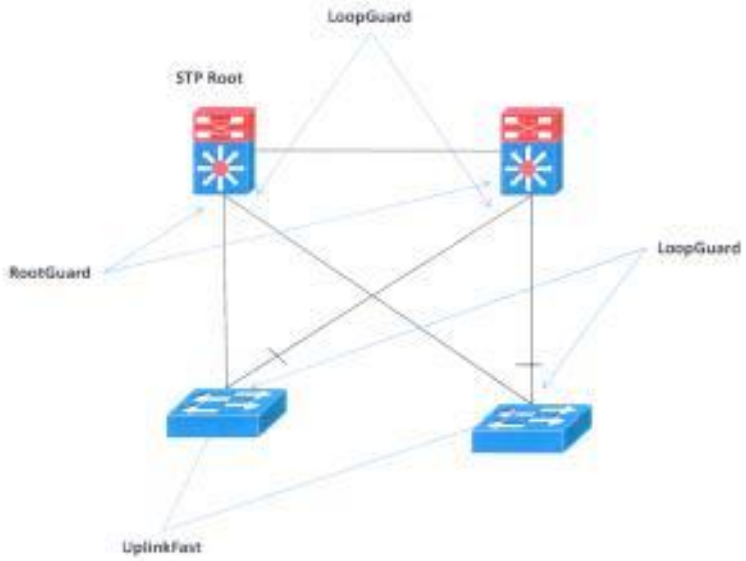


Gráfico N°7 : Ubicación Recomendada de Funcionalidades de STP
Fuente : Cisco Internetwork Design Study Guide
Elaboración : Sybex

Lazo de Guardia es implementado en los puertos de capa 2, puertos entre los conmutadores de distribución, y en los puertos de enlace ascendente desde los conmutadores de acceso hacia los conmutadores de distribución.

Guardia Raíz se configura en los puertos de los conmutadores de distribución que dan el frente a los conmutadores de acceso.

Enlace de Subida Rápido se implementa en los puertos del enlace ascendente de los conmutadores de acceso hacia los conmutadores de distribución.

Guardia de Protocolo de Unidad de Datos de Puente o Guardia Raíz es configurado en los puertos de los conmutadores de acceso hacia los dispositivos finales, que tienen configurado Puerto Rápido.

El protocolo UDLD permite monitorear la configuración física de los cables y detectar cuando un enlace unidireccional existe. Cuando un enlace unidireccional es detectado, UDLD inhabilita el puerto LAN afectado.

Dependiendo de los requisitos de seguridad en una organización, se puede utilizar seguridad en puertos para restringir el tráfico en un puerto de entrada al limitar las direcciones MAC permitidas para enviar el tráfico en el puerto.

2.2.5 Enlaces Troncales

Un enlace troncal, es un enlace punto a punto entre dos dispositivos de red que transportan el tráfico de múltiples redes virtuales. Los enlaces troncales se implementan en la interconexión entre las capas de acceso y distribución.

En la práctica actual se recomienda utilizar el protocolo IEEE 802.1Q. La extensión de Cisco de 802.1Q se utiliza para evitar problemas de seguridad relacionados con el 802.1Q No etiquetado de la red virtual nativa. Para la red virtual nativa es asignado a un identificador (ID) no utilizada, la opción de red virtual nativa se utiliza para evitar el Salto de Red Virtual. (Salto de Red Virtual es un ataque usando un doble encapsulado de paquetes 802.1Q). Si el atacante tiene un conocimiento especifico de la red virtual nativa 802.1Q).

Protocolo Troncal de Red Virtual (VTP) es un protocolo que permite a los administradores de red administrar centralizadamente la base de datos de VLAN. El modo VTP transparente es ahora una práctica recomendada debido a que disminuye la posibilidad de un error de operación.

VTP versión 3 es compatible con la administración centralizada de redes virtuales en una red conmutada. VTP sólo se ejecuta en las troncales y ofrece los siguientes cuatro modos:

- *Servidor:* Actualizaciones de los clientes y servidores. El conmutado que actúa como servidor VTP propaga la base de datos de las redes virtuales a los conmutadores clientes.

- *Cliente*: Recibe actualizaciones, pero no puede hacer cambios.

- *Transparente:* No participa en el dominio VTP. Permite pasar a través de el las actualizaciones.

- *Apagado:* Ignora las actualizaciones VTP.

Con VTP, al configurar una nueva red virtual en un conmutador en el modo de servidor VTP, la red virtual se distribuye a través de todos los conmutadores en el dominio VTP. Esta redistribución reduce la necesidad de configurar la misma red virtual en todos los conmutadores.

Con las redes jerárquicas que extienden las redes virtuales a través de la capa de distribución, hay poca necesidad de compartir una base de datos de redes virtuales. En el diseño del campus se recomienda, que la misma red virtual no debe aparecer en dos conmutadores de la capa de acceso. Agregar y quitar las redes virtuales no es generalmente una práctica frecuente de gestión de red. En la mayoría de los casos, las redes virtuales se definen una vez durante la instalación del conmutador con pocas modificaciones adicionales a la base de datos de redes virtuales en un conmutador de la capa de acceso. Los beneficios de la propagación dinámica de la información de redes virtuales a través de la red no vale la pena la posibilidad de un comportamiento inesperado debido a un error de operación. Por estas razones, el modo VTP transparente es el modo recomendado de configuración.

2.2.5.1 Protocolo de enlace troncal dinámico.

El Protocolo de Enlace Troncal Dinámico (DTP) permite a los puertos de un conmutador negociar el método troncal con otro dispositivo y permite automáticamente a un enlace convertirse en un enlace troncal.

Con los dispositivos Cisco, hay cinco modos de puerto en Capa 2:

- *Troncal:* Pone el puerto en modo troncal permanente y negocia para convertir el enlace en una troncal. El puerto se convierte en un puerto troncal, incluso si el puerto vecino no está de acuerdo con el cambio.

- *Deseable:* Activamente intenta formar una troncal, sujeto a un acuerdo con el conmutador vecino. El puerto se convierte en un puerto troncal si el puerto del conmutador vecino está activado, deseables, o modo Auto.

- *Auto:* Hace que el puerto este dispuesto a convertir el enlace en un puerto troncal. El puerto se convierte en un puerto troncal si el puerto del conmutador vecino está encendido o en modo deseable.

- *Acceso*: Este es el modo de acceso en el software Cisco IOS que especifica que el puerto nunca se convierte en una troncal, incluso si el vecino trata. Este modo pone el puerto LAN en el modo de no troncal permanente.

- *No Negociable:* Evita que el puerto genere tramas de DTP. Se debe configurar el puerto vecino manualmente como un puerto troncal para establecer un enlace troncal.

Con los dispositivos de Cisco, hay tres tipos de encapsulación de puertos troncales Ethernet:

ISL: Utiliza encapsulación Enlace Inter Conmutador (ISL) en la encapsulación de los paquetes que pasan por el enlace troncal.

Dot1q: Utiliza la encapsulación 802.1Q en los paquetes que pasan por el enlace troncal.

Negociación: Especifica que la negociación del puerto LAN con el puerto vecino LAN para convertirse en un ISL (preferido) o una troncal 802.1Q dependiendo de las capacidades de los puertos LAN vecinos.

En el modo de troncal, el tipo de encapsulación de la troncal, y las capacidades del hardware de los dos puertos LAN, determinan si un enlace se convierte en una troncal ISL o 802.1Q. Una práctica común es configurar los dos extremos de la troncal deseable. Esto tiene el beneficio operativo de proporcionar una clara indicación de

una conexión troncal funciona con el comando Show y es la recomendación general para troncales DTP.

Una práctica alternativa es establecer un lado del enlace (normalmente, la capa de acceso) para Auto y el otro extremo (por lo general la capa de distribución) a la deseable. Esta configuración permite la formación automática del enlace troncal, con DTP se ejecutan en la interconexión para la protección contra algunos raros casos de fallo de hardware y errores de configuración de software.

2.2.5.2 Ether Canales.

Un Ether Canal agrupa varios enlaces individuales de Ethernet en un único enlace lógico que proporciona el ancho de banda agregado de hasta ocho enlaces físicos. Los Ether canales se implementan entre la distribución y el núcleo y en la interconexión de núcleo a núcleo incrementando la disponibilidad y el ancho de banda. La agregación de enlaces con Ether canales se utiliza para proporcionar redundancia de enlaces y evitar un solo punto de falla, adicionalmente para reducir la complejidad, porque una única entidad lógica reduce el número de vecindades de capa 3 en comparación con múltiples enlaces en paralelo.

Ether canales también proporciona una optimización de STP al permitir que todos los puertos sean colocados para en el modo de renvio. El STP ve al Ether canal como un solo enlace lógico.

Ether canal crea canales que contienen hasta ocho enlaces paralelos entre los conmutadores. Si los canales están en interfaces en diferentes tarjetas de línea física, hay una mayor disponibilidad, ya que el fracaso de una tarjeta de línea única no causa una pérdida total de conectividad.

Hay dos variantes para el mecanismo de control para Ether canales: el pre estándar de Cisco que utiliza el Protocolo de Agregación de Puertos (PAgP), y el IEEE 802.3ad basado en el Protocolo de Control de Agregación de Enlaces (LACP). PAgP y LACP no interactúan entre si.

Puede configurar manualmente un conmutador en PAgP en un lado y LACP en el otro lado en el modo encendido/encendido. Cuando se hace esto, los puertos no negocian, y por lo tanto no hay tráfico de negociación entre los puertos.

Al conectar un dispositivo con software de Cisco IOS con un dispositivo de sistema operativo de Cisco Catalyst se debe asegurar que el PAgP utilizado para el establecimiento de Ether canales se coordinan. Los valores predeterminados son diferentes para un dispositivo con software Cisco IOS y un dispositivo de sistema operativo Catalyst. Como práctica recomendada, los dispositivos de sistema operativo Catalyst deben de tener PAgP desactivado cuando se conecta a un dispositivo de software Cisco IOS, si los Ether canales no están configurados. Si se desea utilizar los Ether canales con PAgp configure ambos lados de la interconexión en deseable.

La agregación de puertos debe ser desactivada cuando no son necesarios. La agregación de puertos puede más efectivamente ser controlado mediante la desactivación de las interfaces que se conectan a los usuarios finales.

2.2.5.3 Protocolo de Agregación de Puertos.

El Protocolo de Agregación de Puertos (PAgP) es uno de los mecanismos de control para Ether canales. PAgP tiene cuatro modos relacionados a la formación automática de paquetes de link de los enlaces y las interconexiones redundantes de conmutador a conmutador.

- *Encendido:* Este modo forza a los puertos LAN para troncalizarse incondicionalmente. En el modo de encendido, un Ether canal es utilizable sólo cuando existe un grupo de puertos de LAN en el modo encendido que es conectado a otro grupo de puertos de LAN en el modo encendido. Porque en los puertos configurados en el modo de no negociar, no se produce el tráfico de negociación entre los puertos.

- *Deseable:* Coloca un puerto en un estado de negociación activa, en la que el puerto comienza negociaciones con otros puertos mediante el envio de paquetes PAgP. Este modo no es soportado cuando los miembros del Ether canal están en diferentes conmutadores de apilamiento de conmutadores (Pila Cruzada de Ether Canal).

- *Auto:* Coloca un puerto en un estado de negociación pasiva, en la que el puerto responde a paquetes PAgP que recibe, pero no se inicia la negociación de paquetes PAgP. Este ajuste reduce al mínimo la transmisión de paquetes de PAgP. Este modo no está soportado para la los miembros del Ether canal que están en diferentes conmutadores de la pila de conmutadores (Pila Cruzada de Ether Canal).

- *Apagado:* No se convierte en un miembro.

- Para los Ether canales de capa 2, una configuración deseable / deseable, se recomienda para que PAgP se ejecute a través de todos los miembros del conjunto, asegurando que el fallo de un enlace individual no se traducirá en una falla de STP.

2.2.5.4 Protocolo de Control de Agregación de Enlaces.

El Protocolo de Control de Agregación de Enlaces (LACP) es otro mecanismo de control para Ether Canales. LACP tiene cuatro modos de relativos con la formación automática de paquetes para la interconexión redundante de conmutadores a conmutadores:

- *Encendido:* Este modo se forza a un puerto LAN para canalizar incondicionalmente. En el modo de encendido, un Ether Canal es utilizable

sólo cuando existe un grupo de puertos de LAN en el modo encendido se conectado a otro grupo de puertos de LAN en el modo encendido. Debido a que los puertos configurados en el modo de encendido no negocian, no hay tráfico de negociación entre los puertos.

- *Activo:* En este modo LACP coloca los puertos en un estado activo de negociación, en la que el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP.

- *Pasivo:* En este modo LACP coloca los puertos en un estado pasivo de negociación, en la que el puerto responde a los paquetes LACP que recibe pero no inicia LACP negociación.

- Apagado: No se convierte en un miembro LACP.

2.2.6 Sobresuscripción y Ancho de Banda.

Las redes habituales de campus han sido diseñadas con exceso de demanda, la recomendación de la regla de sobresuscripción de datos es de 20:1 para los puertos de acceso en el enlace ascendente de la capa de acceso a la capa de distribución. La recomendación es de 4:1 para la capa de distribución a la capa del núcleo. Al utilizar estas relaciones de sobre subscripción, la congestión puede ocurrir con poca frecuencia en los enlaces ascendentes. Calidad de servicio es requerida en ciertas

ocasiones. Si la congestión ocurre frecuente, el diseño no tiene el suficiente ancho de banda de subida.

La capacidad de ancho de banda de la capa de acceso aumenta a razón de 1Gbps, múltiplos de 1 Gbps, y hasta 10Gbps, en la agregación el ancho de banda en los enlaces ascendentes de distribución hasta el núcleo son en muchos Gigabit Ethernet Ether canales, en enlaces de 10 Gigabit Ethernet, y en enlaces de 10 de Gigabit Ether canales.

2.2.7 Gestión de Ancho de Banda con Ether canales.

El ancho de banda de la capa de distribución hacia el núcleo aumenta, la sobresuscripción hacia la capa de acceso y algunas decisiones de diseño deben hacerse, simplemente añadiendo más enlaces ascendentes entre la distribución y la capa de núcleo conduce a más relaciones con sus pares en capa 3, con un incremento asociado de las cabeceras de los paquetes.

Los Ether canales pueden reducir el numero de pares mediante la creación de la interfaz lógica única. Sin embargo, se debe tener en cuenta algunas consideraciones, acerca de cómo los protocolos de enrutamiento reaccionará a la falla de un link.

Si el protocolo de enrutamiento OSPF se ejecuta en un conmutador con un software basado en Cisco IOS, se dará cuenta de la caída de un enlace e incrementara el costo

de un enlace, y aumentará el costo del enlace. El tráfico se desviara, y este diseño conduce a un evento de convergencia.

Si el protocolo de enrutamiento OSPF se ejecuta en un conmutador con un software hibrido Cisco IOS, no va a cambiar costo del enlace. Porque se seguirá utilizando el Ether Canal, esto puede conducir a una sobrecarga en el resto de los enlaces pero OSPF sigue dividiendo por igual en el tráfico a través de los canales con anchos de banda diferentes.

El protocolo de enrutamiento EIGRP no puede cambiar costo del enlace, ya que el protocolo ve los costos de extremo a extremo. Este diseño también puede sobrecargar los enlaces restantes. La característica Enlaces Min Ether Canales es compatible con Ether canales LACP. Esta característica le permite configurar el número mínimo de puertos que pertenecen al canal que deben estar en el estado de enlace activo y envuelto en el Ether canal. Se puede utilizar la función Ether Canal Enlaces-Min para evitar el bajo ancho de banda de los Ether canales LACP y que se conviertan en un enlace activo.

2.3 Consideraciones de Diseño en Enrutadores

2.3.1 Enrutamiento

Es posible que los usuarios de una red no estén al tanto de la presencia de numerosos enrutadores en su propia red LAN o en el Internet. Los usuarios esperan poder

acceder a las páginas Web, enviar mensajes de correo electrónico y descargar música, ya sea si el servidor al que están accediendo está en su propia red o en otra red del otro lado del mundo.

Un enrutador conecta múltiples redes. Esto significa que tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un enrutador recibe un paquete IP en una interfaz, determina qué interfaz usar para renviar el paquete hacia su destino. La interfaz que usa el enrutador para renviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro enrutador que se usa para llegar a la red de destino.

Generalmente, cada red a la que se conecta un enrutador requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de Redes de área local (LAN) y Redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como PC, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa.

La principal responsabilidad de un enrutador es dirigir los paquetes destinados a redes locales y remotas mediante:

- La determinación del mejor camino para enviar paquetes.
- El renvío de los paquetes a su destino.

El enrutador usa su tabla de enrutamiento para determinar el mejor camino para renviar el paquete. Cuando el enrutador recibe un paquete, examina su dirección IP de destino y busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del enrutador. La tabla de enrutamiento también incluye la interfaz que se utilizará para renviar el paquete. Cuando se encuentra una coincidencia, el enrutador encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida. Luego, el paquete se renvía hacia su destino.

2.3.1.1 Tipos de Enrutamiento

Los enrutadores usan protocolos de rutas estáticas y de enrutamiento dinámico para detectar redes remotas y crear sus tablas de enrutamiento.

Los protocolos de enrutamiento dinámico se han usado en redes desde comienzos de la década del ochenta. La primera versión (V1) de RIP se lanzó en 1982, pero algunos de los algoritmos básicos dentro del protocolo ya se usaban en ARPANET en 1969. Debido a la evolución de las redes y a su complejidad cada vez mayor, han surgido nuevos protocolos de enrutamiento. Uno de los primeros protocolos de enrutamiento fue el Protocolo de Información de Enrutamiento (RIP). RIP ha evolucionado a una nueva versión, el RIPv2. Sin embargo, la nueva versión (V2) aún no se escala a implementaciones de redes más extensas se limita a 15 saltos. Para abordar las necesidades de redes más amplias, se desarrollaron dos protocolos de enrutamiento avanzados: El Protocolo Abierto del Primer Camino Corto (OSPF) y Sistema

Intermediario a Sistema Intermediario (IS-IS). Cisco desarrolló el Protocolo de Enrutamiento de Puerta de Enlace Interior (IGRP) y el IGRP mejorado (EIGRP), que también se adapta bien en implementaciones de redes más grandes.

Los protocolos de enrutamiento dinámicos se usan para facilitar el intercambio de información de enrutamiento entre los enrutadores. Estos protocolos permiten a los enrutadores compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento.

Los protocolos de enrutamiento determinan el mejor camino hacia cada red, que luego se agrega a la tabla de enrutamiento. Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico es que los enrutadores intercambian información de enrutamiento cuando se produce un cambio de topología. Este intercambio permite a los enrutadores obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, el costo de usar protocolos de enrutamiento dinámico es dedicar parte de los recursos de los enrutadores para la operación del protocolo, incluso el tiempo de la Unidad Central de Procesos (CPU) y el ancho de banda del enlace de red. Pese a los beneficios del

enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar. En algunas ocasiones el enrutamiento estático es más apropiado, mientras que en otras, el enrutamiento dinámico es la mejor opción, esta selección adecuada del mismo recae en el diseñador de la red.

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la selección de los mejores caminos que realiza el protocolo. El propósito de un protocolo de enrutamiento incluye:

- Descubrir redes remotas.
- Mantener la información de enrutamiento actualizada.
- Escoger el mejor camino hacia las redes de destino.
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar accesible.

2.3.1.2 Ventajas y Desventajas del Enrutamiento Estático

En la tabla se comparan directamente las características del enrutamiento dinámico y estático. A partir de esta comparación, podemos enumerar las ventajas de cada método de enrutamiento. Las ventajas de un método son las desventajas del otro.

2.3.1.2.1 Ventajas del Enrutamiento Estático:

A continuación se indica algunas ventajas del enrutamiento estático.

- El procesamiento de la CPU es mínimo.
- Es más fácil de comprender para el administrador.
- Es fácil de configurar.

2.3.1.2.2 Desventajas del Enrutamiento Estático:

A continuación se indica algunas desventajas del enrutamiento estático.

- La configuración y el mantenimiento son prolongados.
- La configuración es propensa a errores (por parte de los administradores), especialmente en redes extensas.
- Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
- No se adapta bien a las redes en crecimiento; el mantenimiento se torna cada vez más complicado.
- Requiere un conocimiento completo de toda la red por parte del administrador para una correcta implementación.

2.3.1.3 Ventajas y Desventajas del Enrutamiento Dinámico

2.3.1.3.1 Ventajas del Enrutamiento Dinámico:

A continuación se indica algunas ventajas del enrutamiento dinámico.

- El administrador tiene menos trabajo en el mantenimiento de la configuración cuando agrega o quita redes.
- Los protocolos reaccionan automáticamente a los cambios de topología.
- La configuración es menos propensa a errores.
- Es más escalable, el crecimiento de la red normalmente no representa un problema.

2.3.1.3.2 Desventajas del Enrutamiento Dinámico:

A continuación se indica algunas desventajas del enrutamiento dinámico.

- Se utilizan recursos del enrutador (ciclos de CPU, memoria y ancho de banda del enlace).
- El administrador requiere más conocimientos para la configuración, verificación y resolución de problemas.

Al hablar de protocolos de enrutamiento dinámico requerimos mencionar a los sistemas autónomos, un sistema autónomo (AS), conocido también como dominio de enrutamiento, es un conjunto de enrutadores que se encuentran bajo una administración común. Algunos ejemplos típicos son la red interna de una empresa y la red de un proveedor de servicios de Internet. Debido a que Internet se basa en el concepto de sistema autónomo, se requieren dos tipos de protocolos de enrutamiento: protocolos de enrutamiento interior y exterior. Estos protocolos son:

Protocolos de puerta de enlace interior (IGP): se usan para el enrutamiento de sistemas intra autónomos (el enrutamiento dentro de un sistema autónomo).

Protocolos de puerta de enlace exterior (EGP): se usan para el enrutamiento de sistemas inter autónomos (el enrutamiento entre sistemas autónomos).

Los protocolos de puerta de enlace interior (IGP) pueden clasificarse en dos tipos:

- Protocolos de enrutamiento vector distancia
- Protocolos de enrutamiento de Estado de Enlace

2.3.2 Protocolos de Enrutamiento Vector Distancia

"Vector distancia" significa que las rutas se publican como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el enrutador del siguiente salto o la interfaz de salida. Los protocolos vector distancia generalmente usan el algoritmo Bellman-Ford para la determinación del mejor camino.

Algunos protocolos vector distancia envian en forma periódica tablas de enrutamiento completas a todos los vecinos conectados. En las redes extensas, estas actualizaciones de enrutamiento pueden llegar a ser enormes y provocar un tráfico importante en los enlaces.

Los protocolos vector distancia funcionan mejor en situaciones donde:

- La red es simple y plana y no requiere de un diseño jerárquico especial,
- Los administradores no tienen suficientes conocimientos como para configurar protocolos de estados de enlace y resolver problemas en ellos,
- Se están implementando tipos de redes específicos, como las redes concentrador y hablante.
- No es motivo de preocupación un tiempo convergencia rápida

2.3.3 Protocolos de Enrutamiento de Estado de Enlace.

A diferencia de la operación del protocolo de enrutamiento vector distancia, un enrutador configurado con un protocolo de enrutamiento de estado de enlace puede crear una "vista completa" o topología de la red al reunir información proveniente de todos los demás enrutadores, el uso de un protocolo de enrutamiento de estado de enlace es como tener un mapa completo de la topología de la red. Un enrutador de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar el mejor camino hacia todas las redes de destino en la topología.

Como algunos protocolos de enrutamiento vector distancia, los enrutadores envían actualizaciones periódicas de su información de enrutamiento a sus vecinos. Los

protocolos de enrutamiento de estado de enlace no usan actualizaciones periódicas. Luego de que la red ha convergido, la actualización del estado de enlace sólo se envía cuando se produce un cambio en la topología.

Los protocolos de estados de enlace funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, y por lo general ocurre en redes extensas.
- Los administradores conocen a fondo el protocolo de enrutamiento de estado de enlace implementado.
- Es crucial la rápida convergencia de la red.

En nuestro caso seleccionamos a los protocolos de estado de enlace, como protocolo de enrutamiento ya que es crucial la rápida convergencia de la red.
A los protocolos de enrutamiento de estado de enlace también se les conoce como protocolos de Primer Camino Corto y se desarrollan en torno del algoritmo Ruta Más Corta Primero (SPF) de Edsger Dijkstra.

Al algoritmo de Dijkstra se le llama comúnmente algoritmo Ruta Más Corta Primero (SPF). Este algoritmo acumula costos a lo largo de cada ruta, desde el origen hasta el destino. Si bien al algoritmo de Dijkstra se le conoce como el algoritmo Ruta Más Corta Primero, éste es de hecho el objetivo de cada algoritmo de enrutamiento.

Los enrutadores configurados con protocolos de enrutamiento de estado de enlace llevan a cabo el siguiente proceso genérico de enrutamiento de estado de enlace para alcanzar un estado de convergencia:

- Cada enrutador obtiene información sobre sus propios enlaces, sus propias redes conectadas directamente. Esto se realiza al detectar que una interfaz se encuentra en el estado activado.
- Los enrutadores de estado de enlace realizan intercambio de paquetes de saludo con otros enrutadores de estado de enlace en redes conectadas directamente.
- Cada enrutador crea un Paquete de Estado de Enlace (LSP) que incluye el estado de cada enlace directamente conectado. Esto se realiza registrando toda la información pertinente acerca de cada vecino, que incluye el identificador (ID) del vecino, el tipo de enlace y el ancho de banda.
- Cada enrutador satura con el LSP a todos los vecinos, que luego almacenan todos los LSP recibidos en una base de datos. Los vecinos luego saturan con los LSP a sus vecinos hasta que todos los enrutadores del área hayan recibido los LSP. Cada enrutador almacena una copia de cada LSP recibido por parte de sus vecinos en una base de datos local.
- Cada enrutador utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino. El enrutador tiene ahora un mapa completo de todos los destinos de la topología y las rutas

para alcanzarlos. El algoritmo SPF se utiliza para construir el mapa de la topología y determinar el mejor camino hacia cada red.

Las siguientes son algunas ventajas de los protocolos de enrutamiento de estado de enlace comparados con los protocolos de enrutamiento vector distancia.

- *Crean un mapa topológico:* Los protocolos de enrutamiento de estado de enlace crean un mapa topológico o árbol SPF de la topología de red. Los protocolos de enrutamiento vector distancia no tienen un mapa topológico de la red. Los enrutadores que implementan un protocolo de enrutamiento vector distancia sólo tienen una lista de redes, que incluye el costo (distancia) y los enrutadores del siguiente salto (dirección) a dichas redes. Debido a que los protocolos de enrutamiento de estados de enlace intercambian estados de enlace, el algoritmo SPF puede crear un árbol SPF de la red. Al utilizar el árbol SPF, cada enrutador puede determinar en forma independiente la ruta más corta a cada red.
- *Convergencia rápida:* Al recibir un Paquete de Estado de Enlace (LSP), los protocolos de enrutamiento de estado de enlace saturan de inmediato con el LSP todas las interfaces excepto la interfaz desde la que se recibió el LSP. Un enrutador que utiliza un protocolo de enrutamiento vector distancia necesita procesar cada actualización de enrutamiento y actualizar su tabla de enrutamiento antes de saturarlas a otras interfaces, incluso con actualizaciones

generadas por eventos. Se obtiene una convergencia más rápida para los protocolos de enrutamiento de estado de enlace.

- *Actualizaciones desencadenadas por eventos:* Después de la saturación inicial de los LSP, los protocolos de enrutamiento de estado de enlace sólo envían un LSP cuando hay un cambio en la topología. El LSP sólo incluye la información relacionada con el enlace afectado. A diferencia de algunos protocolos de enrutamiento vector distancia, los protocolos de enrutamiento de estado de enlace no envían actualizaciones periódicas.
- *Diseño jerárquico:* Los protocolos de enrutamiento de estado de enlace, como OSPF e IS-IS utilizan el concepto de áreas. Las áreas múltiples crean un diseño jerárquico para redes y permiten un mejor agregado de rutas (sumarización) y el aislamiento de los problemas de enrutamiento dentro del área.

2.3.3.1 Requisitos de un Protocolo de Estado de Enlace

Los protocolos de enrutamiento de estado de enlace modernos están diseñados para minimizar los efectos en la memoria, el CPU y el ancho de banda. La utilización y configuración de áreas múltiples puede reducir el tamaño de las bases de datos de estado de enlace. Las áreas múltiples también pueden limitar el grado de saturación de información de un dominio de enrutamiento y enviar los LSP sólo a aquellos enrutadores que los necesitan.

Por ejemplo, cuando hay un cambio en la topología, sólo los enrutadores del área afectada reciben el LSP y ejecutan el algoritmo SPF. Esto puede ayudar a aislar un enlace inestable en un área específica en el dominio de enrutamiento.

- *Requisitos de memoria:* Los protocolos de enrutamiento de estado de enlace normalmente requieren más memoria, más procesamiento de CPU y en ocasiones un mayor ancho de banda que los protocolos de enrutamiento vector distancia. Los requisitos de memoria responden a la utilización de bases de datos de estados de enlace y la creación del árbol SPF.
- *Requisitos de procesamiento:* Los protocolos de estado de enlace también pueden requerir un mayor procesamiento de CPU que los protocolos de enrutamiento vector distancia. El algoritmo SPF requiere un mayor tiempo de CPU que los algoritmos vector distancia, como Bellman-Ford, ya que los protocolos de estado de enlace crean un mapa completo de la topología.
- Requisitos de ancho de banda: La saturación de paquetes de estado de enlace puede ejercer un impacto negativo en el ancho de banda disponible en una red. Si bien esto sólo debería ocurrir durante la puesta en marcha inicial de los enrutadores, también podría ser un problema en redes inestables.

2.3.3.2 Protocolo Abierto Primero la Ruta mas Corta.

Frecuentemente llamado OSPF es un protocolo de enrutamiento jerárquico de puerta de enlace interior o IGP, que usa el algoritmo de Dijkstra de estado enlace (LSA) para

calcular la ruta más corta posible. Usa el costo como su medida de métrica. Además, construye una base de datos de estado de enlace (LSDB) idéntica en todos los enrutadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Sistema Intermediario – Sistema Intermediario IS-IS, es otro protocolo de enrutamiento dinámico de estado de enlace, es más común en grandes proveedores de servicio. Puede operar con seguridad usando el Algoritmo de Resumen del Mensaje 5 (MD5) para autentificar a sus vecinos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Soporta Mascara de longitud Variable (VLSM) o Enrutamiento entre Dominios sin Clases (CIDR) desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área principal que forma la parte central de la red y donde hay otras áreas conectadas a ella. Las rutas entre diferentes áreas circulan siempre por el área principal, por lo tanto todas las áreas deben conectar con a la principal.

Los enrutadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un

segmento de red Ethernet los enrutadores eligen a un enrutador designado (DR) y un enrutador designado secundario (BDR) que actúan como concentradores para reducir el número de adyacencias que debe formar cada enrutador. OSPF puede usar tanto multidifusión como unidifusión para enviar paquetes de helo y actualizaciones de estado de enlace. Las direcciones de multidifusión usadas son 224.0.0.5 y 224.0.0.6.

2.3.3.2.1 Tipos de paquetes de OSPF

OSPF tiene cinco tipos diferentes de paquetes LSP de OSPF. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

Saludo: los paquetes de saludo se utilizan para establecer y mantener la adyacencia con otros enrutadores OSPF.

DBD: el paquete de Descriptores de bases de datos (DBD) incluye una lista abreviada de la base de datos de estados de enlace del enrutador emisor y es utilizado por los enrutadores receptores para realizar una comparación con la base de datos de estado de enlaces. Cada enrutador OSPF mantiene una base de datos de estados de enlace que contiene las LSA recibidas por parte de todos los demás enrutadores. Una vez que un enrutador recibió todas las LSA y creó su base de datos de estado de enlace local, OSPF utiliza el algoritmo el camino mas corto primero (SPF) de Dijkstra para crear un árbol SPF. El árbol SPF luego se utiliza para completar la tabla de enrutamiento IP con las mejores rutas para cada red.

LSR: los enrutadores receptores pueden entonces solicitar más información acerca de una entrada en la DBD enviando un paquete de solicitud de estado de enlace (LSR).

LSU: los paquetes de actualización de estado de enlace (LSU) se utilizan para responder las LSR y para anunciar nueva información. Las LSU contienen siete tipos diferentes de notificaciones de estado de enlace (LSA). Las actualizaciones de estado de enlace (LSU) son los paquetes utilizados para las actualizaciones de enrutamiento OSPF. La diferencia entre los términos actualización de estado de enlace (LSU) y notificación de estado de enlace (LSA) en ocasiones puede ser confusa. A veces, dichos términos pueden utilizarse indistintamente. Una LSU incluye una o varias LSA y cualquiera de los dos términos puede usarse para hacer referencia a la información de estado de enlace propagada por los enrutadores OSPF.

LSAck: cuando se recibe una LSU, el enrutador envía un acuse de recibo de estado de enlace (LSAck) para confirmar la recepción del paquete LSU.

2.3.3.2.2 Métrica de OSPF

La métrica del OSPF se denomina costo. En el RFC 2328: "Un costo se asocia con el resultado de cada interfaz del enrutador. Dicho costo está configurado por el administrador del sistema, cuanto más bajo sea el costo, más probabilidad hay de que la interfaz sea utilizada para enviar tráfico de datos", observe que el RFC 2328 no especifica los valores que deben utilizarse para determinar el costo. El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el enrutador

hasta la red de destino como el valor del costo. En cada enrutador, el costo de una interfaz se calcula en 10 a la octava potencia dividido por el ancho de banda en bps. Esto se conoce como ancho de banda de referencia. La división de 10 a la octava potencia por el ancho de banda de la interfaz se realiza para que las interfaces con mayores valores de ancho de banda tengan un costo calculado inferior. Recuerde, en las métricas de enrutamiento, la ruta de inferior costo es la ruta preferida (por ejemplo, con RIP, 3 saltos es mejor que 10 saltos). La figura muestra los costos predeterminados de OSPF para varios tipos de interfaces.

Cuadro N° 3
Costo de OSPF para Varios Tipos de Interface

TIPO DE INTERFAZ	COSTO
Fast Ethernet y mas rápidas	1
Ethernet	10
E1	48
T1	64
128 Kbps	781
64 Kbps	1562
56 Kbps	1785

Fuente : Cisco CCNA 1
Elaboración : Cisco Press

2.3.3.2.3 Ancho de Banda de Referencia

El ancho de banda de referencia predeterminado es de 10 a la octava potencia, 100 000 000 bps o 100 Mbps. Esto da como resultado interfaces con un ancho de banda de 100 Mbps y más con el mismo costo de OSPF de 1. El ancho de banda de

referencia puede modificarse para adaptarse a redes con enlaces más rápidos que 100 000 000 bps (100 Mbps) con el comando "auto-cost reference-bandwidth" de OSPF. Cuando este comando es necesario, se recomienda su utilización en todos los enrutadores para que la métrica de enrutamiento de OSPF se mantenga uniforme.

2.4 Protocolos de Administración de Red.

La adecuada administración de la red es un componente crítico de una red eficiente. Los administradores de red necesitan herramientas para monitorear la funcionalidad de los dispositivos de red, las conexiones entre ellos, y los servicios que prestan. Protocolo de Administración Sencilla de Red (SNMP) se ha convertido en el estándar de facto para su uso en soluciones de administración de red y está estrechamente relacionado con el Monitoreo Remoto (RMON) y Administración de Bases de Información (MIB). Cada dispositivo gestionado en la red tiene varias variables que cuantifican el estado del dispositivo.

Se puede monitorear los dispositivos administrados por la lectura de los valores de estas variables, y se puede controlar los dispositivos administrados por la escritura de valores en estas variables.

2.4.1 Arquitectura de Administración de Red

La arquitectura de la administración de red consiste en lo siguientes elementos:

- *Sistema de administración de red (NMS):* Un sistema que ejecuta las aplicaciones que monitorean y controlan los dispositivos administrados. NMS's proporcionan la mayor parte de los recursos de procesamiento y memoria que son necesarios para la gestión de la red.
- *Protocolo de administración de red:* Un protocolo que facilita el intercambio de la información de gestión entre los dispositivos gestionados y el NMS, se incluye en estos protocolos SNMP, MIB y RMON.
- *Los dispositivos administrados:* Un dispositivo (como un enrutador), gestionado por un NMS.
- *Administración de agentes:* Es un software, en los dispositivos administrados, que recoge y almacena la información de la administración, se incluye los agentes SNMP y agentes RMON.
- *Administración de la información:* Los datos que son de interés para la gestión de un dispositivo, normalmente se almacena en las MIB.

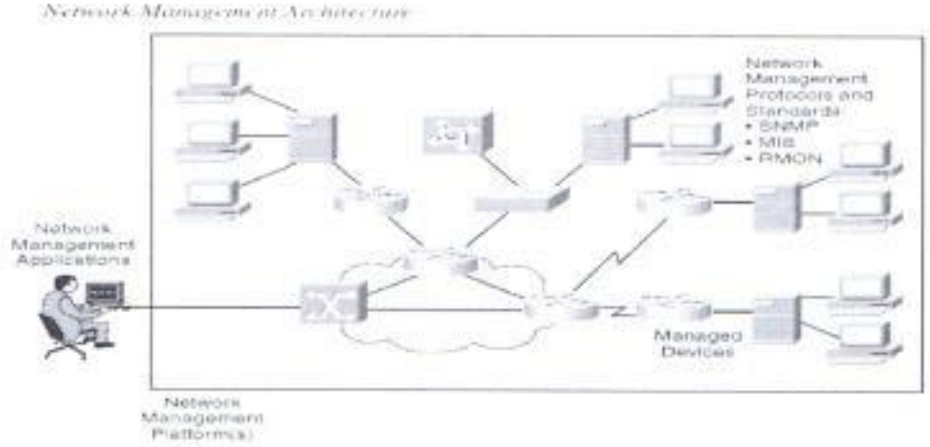


Gráfico N°8 : Arquitectura de Administración de Red
Fuente : Cisco Internetwork Design Study Guide
Elaboración : Sybex

Una variedad de aplicaciones de administración de redes se puede utilizar en un sistema de administración de red; la elección depende de la plataforma de red (por ejemplo, el hardware o sistema operativo). La información de administración reside en los dispositivos de red, los agentes de administración que residen en el dispositivo que recopilan y almacenan datos en una estructura de datos definida y estandarizada conocida como MIB.

Las aplicaciones de administración de red utilizan el protocolo SNMP u otro tipo de protocolo de administración de red para recuperar los datos que recogen los agentes de administración. Los datos recuperados se procesan y típicamente preparados para su visualización con una interfaz de usuario, que permite al operador utilizar una representación gráfica de la red para controlar los dispositivos administrados y el programa de aplicación de administración de red.

2.4.2 Protocolos y Estándares.

2.4.2.1 Protocolo de Administración Sencillo de Red

También conocido como SNMP se ha convertido en el estándar de facto para la administración de la red. SNMP es una solución sencilla que requiere poco código para ponerlo en práctica, lo que permite a los proveedores construir fácilmente los agentes SNMP para sus productos. Además, SNMP es a menudo la base de la arquitectura de administración de red. SNMP define como la información de la administración se intercambia entre las aplicaciones de gestión de redes y agentes de

administración. El Gráfico 10 muestra los términos utilizados en SNMP, que se describen a continuación:

- *Administrador:* El administrador, es una aplicación de administración de red en un NMS, periódicamente encuestas a los agentes SNMP que residen en los dispositivos administrados para los datos, permitiendo así a la información para que se muestre en una interfaz gráfica de usuario en los NMS. Una desventaja de la encuesta periódica SNMP, es el posible retraso entre el momento que se produce un evento y cuando es colectado por el NMS, hay un tiempo de espera entre la frecuencia de sondeo y la utilización de ancho de *banda.*
- *Protocolo SNMP:* SNMP es un protocolo para el intercambio de mensajes. Se utiliza el Protocolo UDP para enviar y recuperar la información de administración, tales como las variables MIB.
- *Dispositivo administrado:* Un dispositivo (como un enrutador), gestionado por el administrador.
- *Los agentes de administración*: Los agentes de gestión SNMP residen en los dispositivos administrados para recoger y almacenar una amplia gama de información sobre el dispositivo y su funcionamiento, responder a los requerimientos del administrador, y generar traps para informar al administrador de determinados eventos. Los Traps SNMP se envían por parte de agentes de gestión al NMS cuando se producen determinados eventos.

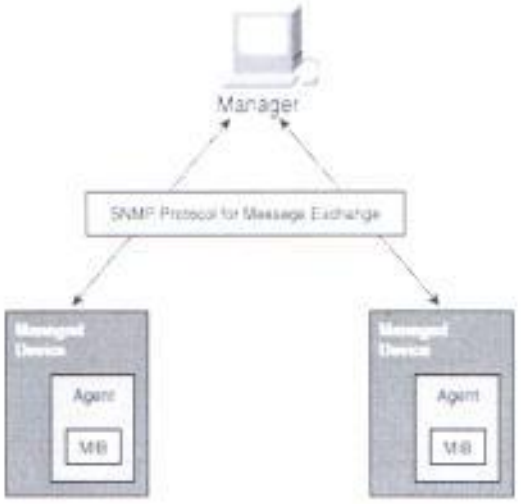


Gráfico N°9 : Protocolo para Intercambio de Información de Administración
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

2.4.2.1.1 SNMPv1.

La versión inicial del SNMP, SNMPv1 se define en el RFC 1157 Protocolo de Administración Sencillo de Redes (SNMP). La simplicidad del protocolo es evidente por el conjunto de operaciones que están disponibles.

Se indican los mensajes básicos de SNMP, que el administrador utiliza para transferir datos de los agentes que residen en los dispositivos administrados, Estos mensajes son: Get Request, Get Next Request, Set Request, Get Response y Trap.

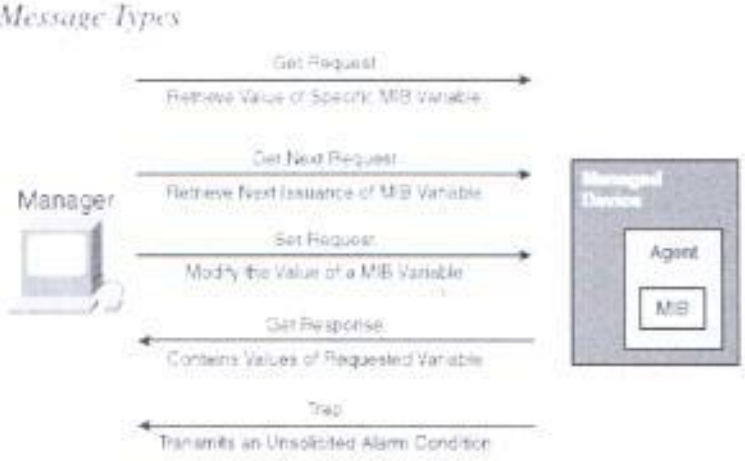


Gráfico N°10 : Tipos de mensajes de SNMP
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

2.4.2.1.2 SMNPv2

SNMPv2 es una versión mejorada, que incluye mejoras en el rendimiento y la comunicación de administrador a administrador. SNMPv2 se introdujo con la RFC 1441. Varios intentos de lograr la aceptación de SNMPv2 se han hecho mediante la liberación experimentales versiones modificadas, conocidas comúnmente como SNMPv2, SNMPv2u, SNMPv1 +, y SNMPv1.5, las cuales no contienen las partes en disputa. Se añadieron los siguientes tipos de mensajes Getbulk y Inform Request.

2.4.2.1.3 SNMPv3

SNMPv3 es la última versión de SNMP, convirtiéndose en un estándar completo, su introducción desplazo a SNMPv1 y SNMPv2 a un estado de histórico. SNMPv3 es

descrito en RFC 3410 hasta el 3415, añade métodos para asegurar una transmisión segura de datos críticos desde los dispositivos administrados.

El SNMPv3 introduce los siguientes niveles de seguridad:

- *NoAuthNoPriv:* Sin autenticación y sin privacidad (encriptación).
- *AuthNoPriv:* Con la autenticación, pero sin privacidad. La autenticación se basa en Hash basado en el Código de autenticación de mensajes, Resumen del Mensaje MD5 o HMAC Algoritmo Seguro de Hash.
- *Authpriv:* Con la autenticación de la forma descrita anteriormente y la privacidad mediante el cifrado de 56 bits (Encadenamiento de Bloque de datos Encriptado estándar).

2.4.2.2 Administración de Bases de Información

También denominadas MIB, son una colección de objetos administrados. Una MIB almacena información, la cual es colectada por el agente local en un dispositivo administrado para posteriormente son requeridos por un protocolo de administración.

Cada objeto en una MIB tiene un único identificador que la aplicación de administración de red usa para identificar y recibir el valor de un objeto específico. Las MIB tienen una estructura igual a un árbol en la cual los objetos similares son agrupados en la misma rama. Por ejemplo contadores interfaces son agrupadas bajo las ramas de las interfaces.

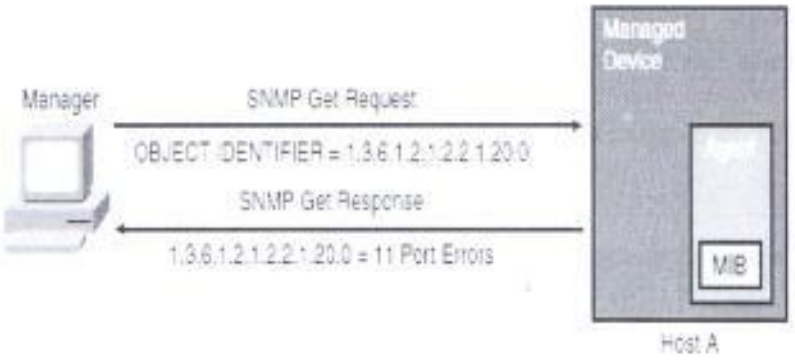


Gráfico N°11 : Ejemplos de Requerimientos de MIB
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

2.4.2.3 Monitoreo Remoto

También conocido como RMON es una MIB que provee soporte para administración proactiva del trafico LAN. El estándar RMON permite que los paquetes y el tráfico en segmentos de LAN a ser monitoreados. RMON da seguimiento de los siguientes elementos:

- Número de paquetes.
- Los tamaños de paquete.
- Broadcast.
- Utilización de la red.
- Errores y condiciones, tales como colisiones de Ethernet.
- Estadísticas de los hosts, incluido los errores generados por los hosts, y cual hosts se comunica con otro.

Las características RMON incluyen vistas históricas de las estadísticas de RMON sobre la base de intervalos definida por el usuario, las alarmas que se basan en umbrales definidos por el usuario y la captura de paquetes basados en filtros definidos por el usuario.

Los agentes RMON pueden residir en enrutadores, conmutadores, concentradores, servidores, computadores, porque RMON puede colectar una porción de datos. Los umbrales de rendimiento pueden ser fijados y reportados, esto ayuda a reducir el tráfico de administración. RMON provee efectivo diagnostico de fallas, ajuste de rendimiento y para planificación de la red.

2.4.2.3.1 RMON 1 y RMON 2.

RMON1 sólo proporciona la visibilidad en el enlace de datos y las capas físicas, los problemas potenciales que se producen en las capas más altas todavía requieren la captura de otras herramientas de decodificación. Debido a las limitaciones de RMON1, RMON2 fue desarrollado para extender la funcionalidad a los protocolos de capas superiores. Como se ilustra en el gráfico 13, RMON2 proporciona visibilidad de la red completa de la capa de red a través de la capa de aplicación.

RMON2 Is an Extension of RMON1

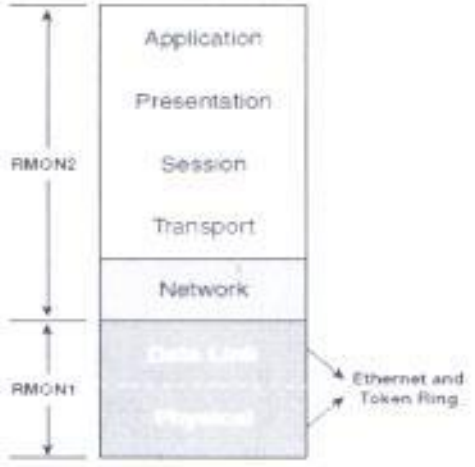


Gráfico N°12 : Descripción de Capas que Cubre RMON 1 y 2
Fuente : Designing Cisco Network Service Architectures
Elaboración : Cisco Press

CAPÍTULO 3

VALORACIÓN DE LOS DISPOSITIVOS DE RED

Y

ANÁLISIS DE RIESGOS

3.1 Levantamiento de Información de los Dispositivos de Red.

Atendiendo a los requerimientos del hospital se realizó el levantamiento de información, la cual se la divide en dos secciones:

- Levantamiento de información de la red LAN.
- Levantamiento de información de la red WAN.

3.1.1 Levantamiento de Información de la Red LAN

En el anexo 1 se adjunta las configuraciones encontradas en los conmutadores de la red, aquí se muestran las salidas de los comandos en los equipos:

Conmutador Cisco 4507R

- Show Version.
- Dir all
- Show running-config

- Show ip route
- Show Vlan
- Show VTP Status
- Show spanning-tree
- Show interfaces status
- Show cdp neighbors

Conmutador Cisco 2960

- Show Version.
- Show running-config
- Show interfaces status
- Show cdp neighbors

3.1.2 Levantamiento de Información de la Red WAN

En el anexo 2 se adjunta las configuraciones encontradas en los enrutadores de la red, aquí se muestran las salidas de los comandos.

Cisco Enrutador 806

- Show version
- Dir all
- Show runn
- Show ip route

- Show ip interface brief.
- Show cdp neighbors

3.2 Funcionalidades Activas en los Dispositivos de Red.

Igual que la sección anterior se dividirá en dos secciones este análisis:

- Funcionalidades activas en los dispositivos activos de la red LAN.
- Funcionalidades activas en los dispositivos activos de la red WAN.

3.2.1 Funcionalidades Activas en los Dispositivos de Red LAN.

3.2.1.1 Conmutador de Núcleo/Agregación

3.2.1.1.1 Conmutador Cisco 4507R.

El conmutador Cisco Catalyst de la serie 4500 proporciona un alto rendimiento, permite un ahorro en seguridad, movilidad, rendimiento de las aplicaciones, video y energía a lo largo de una infraestructura que facilita la virtualización y la automatización. El conmutador Cisco Catalyst de la serie 4500, proporciona rendimiento y escalabilidad.

El Cisco Catalyst 4500 tiene una arquitectura centralizada que permite el renvío de paquetes a altas velocidades características necesarias para un conmutador de núcleo,

la serie E esta disponible en cuatro formatos diferentes: tres ranuras (4503-E), seis ranuras (4506-E), 7-slot (4507R + E/4507R-E), y de 10 ranuras (4510R + E / 4510R-E). La capacidad de recuperación en la serie Cisco Catalyst 4500E incluye un supervisor redundante para los equipos de 10 ranuras y 7 de ranura únicamente, posee ventiladores redundantes, el software es basado en tolerancia a fallos y redundancia 1 +1 en las fuente de alimentación, esta capacidad de recuperación integrada en el hardware y el software minimiza el tiempo de inactividad de la red, ayudando a asegurar la productividad de la empresa.

3.2.1.1.2 Fuentes de Poder

Este dispositivo cuenta con dos fuentes de poder de 1300W, los cuales se utilizan en la modalidad redundante, se realizó el cálculo de la potencia consumida por las tarjetas instaladas en el equipo.

Se observa que las fuentes de poder están al 48% de su capacidad en modalidad redundante, lo que permitiría el soporte en caso de fallo de una de las mismas.

Cuadro N° 4

Potencia proporcionada por la fuente de 1300 Watt

	Porcentaje de Potencia Usada Data	Porcentaje de Potencia usada - PoE	Total Output Power Remaining (W) - Data	Total Output Power Remaining (W) - PoE	Total Output Current for this PSU (A) - Data	Total Output Current for this PSU (A) - PoE	Total Output Current Used (A) - Data	Total Output Current Used (A) - PoE	Total Output Current Remaining (A) -Data	Total Output Current Remaining (A) -PoE
Minima Fuente de Poder										
Única/Redundante 1300 Watt	48.08 %	0.00	1050.0	800.00	87.5	15.3	42.0	0.00	--	15.38
Combinada 1300 Watt	30.28 %	0.00	1667.0	1333.0	138.9	25.6	42.0	0.00	--	25.63

Fuente : Utilidad Cisco Power Calculator
(http://tools.cisco.com/cpc/launch.jsp).
Elaboración: Eduardo Alvarado Unamuno

3.2.1.1.3 Supervisoras

El equipo actualmente cuenta con dos tarjetas supervisoras modelo WS-X4013+, las cuales tienen las siguientes características importantes indicadas en el cuadro N°4, estas tarjetas trabajan en funcionalidades de activo/pasivo y soportan redundancia en caso de falla de la tarjeta activo, la tarjeta pasiva se activa en el tiempo de conmutación es 50 microsegundos con la funcionalidad propietaria de Cisco Stateful Switchover. Esta tarjeta soporta enrutamiento estático y dinámico adicionalmente cuenta con soporte de IPv6.

Cuadro N° 5

Característica de tarjeta controladora WS X4013+

Feature	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-TS	Cisco Catalyst 4500 Series Supervisor Engine II-Plus	Cisco Catalyst 4500 Series Supervisor II-Plus-10GE
Layer 2 - 4 Performance			
Multilayer Switching			
Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP)	Yes	Yes	Yes
EIGRP Stub	Yes	Yes	Yes
Redundant Capable	No	Yes	Yes
CPU (MHz)	266 MHz	266 MHz	667 MHz
NetFlow Support	No	No	No
IP Forwarding Information Base (FIB) Entries	32,000	32,000	32,000
Chassis Support	Cisco Catalyst 4503 and 4503-E Switches Chassis	Cisco Catalyst 4503, 4506, 4507R, 4507R+E, 4510R, and 4510R+E Switches Chassis	Cisco Catalyst 4503, 4506, 4507R, 4507R+E, 4510R, and 4510R+E Switches Chassis
Quality of Service (QoS) Shaping	Non-blocking Gigabit Ethernet ports	Non-blocking Gigabit Ethernet ports	All ports
Broadcast Suppression	Software	Software	Hardware
Multicast Suppression	No	No	Hardware
802.1Q on 802.1Q (Q-in-Q)	No	No	Hardware
Active Redundant Supervisor Engine Uplinks	No	Gigabit Ethernet ports	Any two Gigabit Ethernet ports and the 10 Gigabit Ethernet uplinks

Feature	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-TS	Cisco Catalyst 4500 Series Supervisor Engine II-Plus	Cisco Catalyst 4500 Series Supervisor II-Plus-10GE
Synchronous Dynamic RAM (SDRAM)	256 MB	256 MB	256 MB (512 MB optional upgrade)
Onboard Flash Memory	32 MB	32 MB	64 MB
Active Virtual LANs (VLANs)	2000	2000	2000
Multicast Entries	9000	9000	9000
Spanning Tree Protocol Instances	1500	1500	1500
Switched Virtual Interfaces (SVIs)	1000	1000	1000
Internet Group Management Protocol (IGMP) Snooping	Yes (16,000)	Yes (16,000)	Yes (16,000)
Security/QoS Hardware Entries	32,000	32,000	32,000
Policers	512 egress, 512 ingress	512 egress, 512 ingress	512 egress, 512 ingress

Fuente : Cisco Systems
(http://www.cisco.com/en/US/partner/prod/collateral/modules/ps2797/ps6013/product_data_sheet0900aecd8017a0c5.html).

Elaboración: Cisco Systems

3.2.1.1.4 Tarjetas WS-X4506-GB-T.

Estas tarjetas cumplen la función de realizar la agregación de los conmutadores de acceso dado el tipo de tarjetas supervisoras que posee este conmutador estas se conectan a la matriz de conmutación con un ancho de banda de 6GBps, lo que daría una velocidad de conexión promedio a la matriz de conmutación de cada puerto a 1 Gbps, de esta manera estos puertos no tienen sobresuscripción.

Cuadro N° 6

Característica de tarjeta WS-X4506-GB-T

WS-X4506-GB-T

- 6-port 10/100/1000 and 6-port SFP (any combination of up to 6 ports can be active at one time)
- 10/100/1000 RJ-45 PoE and 1000BASE-X (SFP)
- Cisco IOS Software Release 12.2(20)EWA
- PoE IEEE 802.3af and Cisco prestandard (RJ-45 only)
- Provides full line-rate gigabit switching on all ports
- L2-4 Jumbo Frame support (up to 9216 bytes)
- Designed to give customers the choice of RJ-45 with or without PoE and SFP without incurring extra costs
- Enterprise and commercial: high-performance desktop connectivity and server farms, designed to power IP phones, wireless base stations, video cameras, and other IEEE-compliant appliances
- Service provider: GE small aggregation for DSLAM/PON/mobile data backhaul

Fuente : Cisco Systems
(http://www.cisco.com/en/US/partner/prod/collateral/modules/ps2710/ps5494/product_data_sheet0900aecd802109ea.html).
Elaboración: Cisco Systems

Los seis puertos son duales en esta implementación se utilizan con SFP para conexión en fibra óptica multimodo 62.5/125 micras. Estos puertos se configuran en modo troncal y el encapsulado utiliza 802.1Q para el marcado de las tramas.

3.2.1.1.5 Tarjetas WS-X4424-GB-RJ45.

Este tipo de tarjeta cuenta con 24 puertos 10/100/1000 Rj45, se utilizan para la conexión de estaciones de trabajo y servidores, de acuerdo al tipo de tarjeta supervisoras su conexión a la matriz de conmutación es de 6 Gbps, lo cual da un promedio de conexión de 0,25 Gbps. Las conexiones de estos puertos son con una sobresuscripción de 1:4.

Las funcionalidades configuradas en estos puertos es que los mismos, han sido asignados a la red virtual 1 (Vlan 1 por defecto), y dado que en estos puertos se conectan con estaciones de trabajos y servidores se configura el comando "spanning-tree portfast" para que los puertos ingresen rápidamente en estado de envió.

Dado que este tipo de conmutadores es multicapa se ha configura una SVI (Interface de Conmutador Virtual) para la Vlan 1 con la dirección IP 172.18.1.1, y adicionalmente se ha configurado el comando "ip default-gateway 172.18.1.2" pero dado que en este conmutador no se ha habilitado el enrutamiento con el comando "ip routing" el mismo solo constituye la puerta de enlace por defecto para alcanzar el conmutador.

3.2.1.2 Conmutadores de Acceso

3.2.1.2.1 Conmutador Cisco 2960.

Estos conmutadores se encuentran ubicados en el acceso, sus características principales se describen a continuación en el cuadro N°6, todos los puertos se encuentran ubicados en la red virtual 1 (Vlan por defecto) y dado que en estos puertos se conectan estaciones de trabajo se configura el comando "spanning-tree portfast" para que los puertos ingresen rápidamente en estado de envió.

Cuadro N° 7

Características Principales de Conmutadores Cisco 2960

Performance and Scalability Numbers for All Switch Models		
	Catalyst 2960-S	Catalyst 2960
Forwarding bandwidth	88 Gbps	16 Gbps 32 Gbps (2960G)
Switching bandwidth*	176 Gbps	32Gbps 32 Gbps (2960G)
Flash memory	64 MB	32 MB
Memory DRAM	128 MB	64 MB
Max VLANs	255	255
VLAN IDs	4000	4000
Maximum transmission unit (MTU)	9198 bytes	Up to 9000 bytes
Jumbo frames	9216 bytes	9018 bytes (2960G only)
Forwarding Rate: 64-Byte Packet Cisco Catalyst 2960		
Cisco Catalyst 2960-24TT-L	6.5 mpps	
Cisco Catalyst 2960-24TC-L	6.5 mpps	

Cisco Catalyst 2960-24LT-L	6.5 mpps		
Cisco Catalyst 2960-24PC-L	6.5 mpps		
Cisco Catalyst 2960-48TT-L	10.1 mpps		
Cisco Catalyst 2960-48TC-L	10.1 mpps		
Cisco Catalyst 2960G-24TC-L	35.7 mpps		
Cisco Catalyst 2960G-48TC-L	39.0 mpps		
Resource: Cisco Catalyst 2960-S and 2960	Default	QoS	Dual
Unicast MAC addresses	8000	8000	8000
IPv4 IGMP groups	255	255	255
IPv4 MAC QoS access control entries (ACEs)	128	384	0
IPv4 MAC security ACEs	384	128	256

Fuente : Cisco Systems
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.html
Elaboración: Cisco Systems

Uno de los puertos de enlace ascendente se configura para realizar la conexión al conmutador de núcleo/agregación Cisco 4507R, mientras que para realizar el enlace ascendente hacia los conmutadores localizados en la mismo lugar se utiliza los puertos convencionales, adicionalmente se encontró que en el conmutador de Biblioteca existe un lazo entre los puertos 42 y 48 se adjunta salida del comando show cdp neighbors.

- **Sw1PBBib#sh cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID

Sw1PBCore	Gig 0/1	169	R S I	WS-C4507R Gig 4/4
Sw1PBBib	Fas 0/42	155	S I	WS-C2960- Fas 0/48
Sw1PBBib	Fas 0/48	155	S I	WS-C2960- Fas 0/42

3.2.2 Funcionalidades Activas en los Dispositivos de Red WAN.

3.2.2.1 Enrutador Cisco 806

Se adjunta las características de hardware de los enrutadores Cisco 806 en el cuadro N° 7. Este equipo tiene una capacidad de salida total de 3,58 Mbps calculado considerando paquetes de 64 Bytes.

Se utiliza en esta red enrutamiento estático, la red WAN es una red de capa 2 formada por los equipos de radio. El IOS soportado en este equipo soporta una imagen advance-secutity.

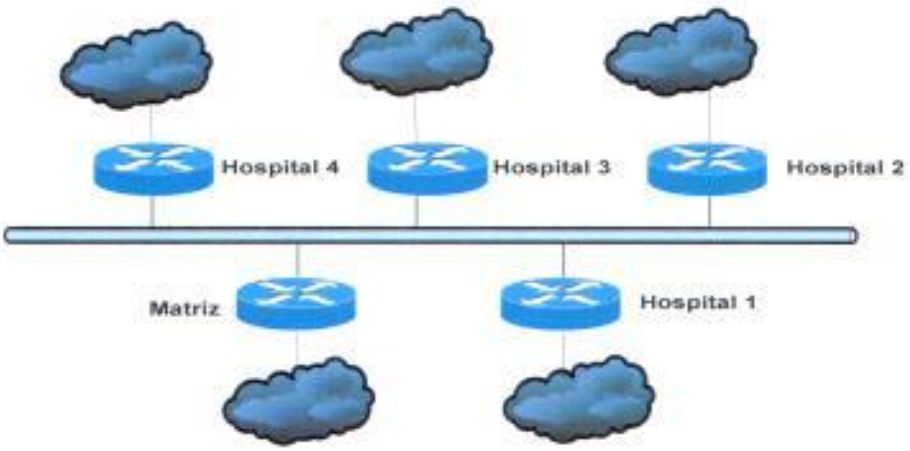


Gráfico N°13 : Vista Lógica de la Red WAN del Hospital
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

Cuadro N° 8

Características de hardware de enrutadores Cisco 806

Hardware specifications	Cisco 806
Processor	MPC 855T RISC
Processor speed	50 MHz
Default DRAM memory	32 MB
Maximum DRAM memory	32 MB
Default Flash memory	8 MB (12 MB on board, 4 MB used with Web Flash for Web configuration tool)
Maximum Flash memory	8 MB
Ethernet (one port WAN, four ports LAN)	10 Mbps
Console	RJ-45
LEDs	10
Hub/No Hub connection switch	Yes
External power supply	Universal 100-240 VAC

Fuente : Cisco Systems
http://www.cisco.com/en/US/products/hw/enrutadores/ps380/products_data_sheet09186a0080088739.html
Elaboración: Cisco Systems

3.2.2.2 Enrutador Cisco 2801

Este equipo tiene una capacidad total de salida de 46,08 Mbps calculado considerando paquetes de 64 Bytes.

Se utiliza en esta red enrutamiento estático, la red WAN es una red de capa 2 formada por los equipos de radio. El IOS de este equipo es Advanced IP Service el cual le soporta enrutamiento dinámico OSPF, EIGRP, RIP.

Se adjunta las características del enrutador 2801.

Cuadro N° 9

Características de hardware de enrutadores Cisco 2801

Cisco 2800 Series	Cisco 2801
Product Architecture	
DRAM	• Default: 128 MB • Maximum: 384 MB
Compact Flash	• Default: 64 MB • Maximum: 128MB
Fixed USB 1.1 Ports	1
Onboard LAN Ports	2-10/100
Onboard AIM (internal) Slot	2
Interface Card Slots	• 4 slots: 2 slots support HWIC, WIC, VIC, or VWIC type modules • 1 slot supports WIC, VIC, or VWIC type modules • 1 slot supports VIC or VWIC type modules

Fuente : Cisco Systems
http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html.
Elaboración: Cisco Systems

3.2.2.3 Enrutador Cisco 831.

Este equipo tiene una capacidad total de salida de 4,35 Mbps calculado considerando paquetes de 64 Bytes. Se utiliza en esta red enrutamiento estático, la red WAN es una red de capa 2 formada por los equipos de radio. El IOS soportado en este equipo soporta una imagen advance-security.

Se adjunta las características del enrutador 831 en el cuadro N° 9.

Cuadro N° 10

Características de hardware de enrutadores Cisco 831

Hardware Specifications	Cisco 831, 836, and 837 Routers
Processor	Motorola RISC
Default DRAM* Memory	64 MB
Maximum DRAM Memory	80 MB
Default Flash* Memory	12 MB
Maximum Flash Memory	24 MB
WAN	• 10BASE-T Ethernet (Cisco 831 router) • ADSL over ISDN-Annex B (Cisco 836 router) • ADSL over POTS-Annex A (Cisco 837 router)
LAN	Four-port 10/100BASE-T with autosensing MDI/MDX for autocrossover
Console Port	This port can be configured to behave as an auxiliary port (virtual AUX) supports modem control for dial backup and out-of-band management
RJ-45	ISDN BRI S/T port which can be configured for ISDN dial backup or out-of-band management (Cisco 836 only)
LEDs	10
External Power Supply	Universal 100-240 VAC

Fuente : Cisco Systems
http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html.
Elaboración: Cisco Systems

3.3 Direccionamiento IP.

Cuadro N° 11

DIRECCIONAMIENTO IP EN VLAN´S DEL HOSPITAL

Equipo	Ubicación	DESCRIPCIÓN						
				MANANGEMENT		USUARIOS		DHCP
		MARCA	MODELO	VLAN	IP	VLAN	IP	ENTREGABLES
1	ADMINISTRACIÓN-FINANCIERA	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.5	13	172.18.4.0/24	11 - 254
2	BIBLIOTECA	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.4	12	172.18.3.0/24	11 - 254
3	CONSULTA EXTERNA	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.9	14	172.18.5.0/24	11 - 254
4	CONSULTA EXTERNA	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.10	14	172.18.5.0/24	11 - 254
5	CONTROL PRINCIPAL	CISCO	Catalyst WS-C4507R	10	172.18.1.1	-	-	-
6	CONTROL PRINCIPAL	CISCO	Catalyst WS-C2960G-48TC - L V02	10	172.18.1.2	11	172.18.2.0/24	11 - 254
7	CONTROL PRINCIPAL	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.3	11	172.18.2.0/24	11 - 254
8	HOSPITALIZACIÓN - Ala Oeste	CISCO	Catalyst WS-C2960-24TC - L V03	10	172.18.1.12	17	172.18.8.0/24	11 - 254
9	HOSPITALIZACIÓN - Ala Este	CISCO	Catalyst WS-C2960-24TC - L V03	10	172.18.1.13	16	172.18.7.0/24	11 - 254
10	HOSPITALIZACIÓN - Ala Este	CISCO	Catalyst WS-C2960S-24TS-L V02	10	172.18.1.14	16	172.18.7.0/24	11 - 254
11	HOSPITALIZACIÓN (UCI)	CISCO	Catalyst WS-C2960-24TC - L V03	10	172.18.1.6	15	172.18.6.0/24	11 - 254
12	LABORATORIO	CISCO	Catalyst WS-C2960-48TC - L V03	10	172.18.1.7	18	172.18.9.0/24	11 - 254
13	LABORATORIO	CISCO	Catalyst WS-C2960-24TC - L V03	10	172.18.1.8	18	172.18.9.0/24	11 - 254
14	PENSIONADO	CISCO	Catalyst WS-C2960-24TC - L V03	10	172.18.1.11	19	172.18.10.0/24	11 - 254
	EQUIPOS MEDICOS	-	-	-	-	20	172.18.11.0/24	11 - 254

Fuente : Datos de investigación
Elaboración: Eduardo Alvarado

El direccionamiento IP utilizado en el hospital es un direccionamiento clase B privado 172.18.0.0/16 al cual se le aplico subredes de 24 bits y asignando una subred a cada red virtual.

3.4 Análisis de Riesgo

El siguiente cuadro indica el análisis de riesgo de las posibles fallas que se puedan presentar en la infraestructura de red.

Cuadro N° 12
Nivel de riesgo

DISPOSITIVO	FALLO	NIVEL DE RIESGO
Conmutador de Núcleo/Agrega. - Cisco 4507R	Tarjeta Procesadora	La falla de una tarjeta procesadora no afecta la operación del equipo ya que cuenta con dos tarjetas procesadoras. **(Bajo)**
	Tarjeta de Enlaces Ascendentes WS-X4506-GB-RJ45	El equipo solo posee una sola tarjeta, el fallo de esta tarjeta dejaría incomunicada a toda la red del Hospital **(Crítico)**
	Fuente de poder de 1300W	Se posee dos fuentes de poder, en caso de falla de una la segunda fuente tiene capacidad para soportar toda la carga, no afecta la operación del equipo **(Bajo)**
	Fallo de Tarjeta WS-X4424-GB-RJ45	El equipo solo posee una tarjeta en caso de falla se perdería conectividad con los servidores **(Crítico)**
	Energía Eléctrica	En caso de falla el hospital posee un UPS y Generador eléctrico. **(Bajo)**
	Circuito Eléctrico	En caso de falla el hospital posee un UPS y Generador eléctrico. **(Bajo)**
	Ventiladores	El equipo posee un juego de ventiladores de respaldo **(Bajo).**
	Carcasa	Este equipo es de clase portadora , su matriz de conmutación pasiva , en caso de fallo la red se quedaría incomunicada **(Crítico)**
	Lazo en la red	El equipo tiene configurado esta protección **(Bajo)**

	IOS	En caso de falla del IOS de la Carcasa el equipo se quedaría sin funcionar **(Crítico)**
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Crítico)**
	Fallos de SFP de enlaces ascendentes	En caso de falla de un SFP de los enlaces ascendentes sé quedaría un piso sin conectividad con la red. **(Medio)**
Conmutador de Acceso	Fuente de poder	En caso de falla de la fuente de poder el equipo se quedaría sin funcionar **(Crítico)**
	Lazo en la red	El equipo tiene configurado esta protección **(Bajo)**
	IOS	En caso de falla del IOS en el equipo se quedaría sin funcionar **(Crítico)**
	Tarjeta principal	En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Crítico)**
	Fallo de SFP de enlaces ascendentes	En caso de falla de un SFP de los enlaces ascendentes sé que daría un piso sin conectividad con la red. **(Medio)**
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Crítico)**
	Energía Eléctrica	En caso de falla el hospital posee un UPS y Generador eléctrico. **(Bajo)**
Fibra Óptica de enlaces ascendentes	Corte	En caso de fallo de la fibra óptica los pisos quedarían incomunicada la red **(Crítico)**
Enrutador 806	Tarjeta Principal	En caso de falla de la tarjeta principal el equipo se quedaría sin funcionar **(Crítico)**
	IOS	En caso de falla del IOS en el equipo se quedaría sin funcionar **(Crítico)**
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar **(Crítico)**
	Energía Eléctrica	En caso de falla el hospital posee un UPS y Generador eléctrico. **(Bajo)**

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

Cuadro N° 13

NIVELES DE RIESGO EN CONMUTADOR DE NÚCLEO

DEPENDIENDO DE LA FALLA DEL COMPONENTE.

CONMUTADOR DE NÚCLEO	EVENTOS CRITICOS	EVENTOS MEDIOS	EVENTOS BAJOS	FRECUENCIA
TARJETA PROCESADORA	0,00	0,00	1,00	1,00
TARJETAS DE ENLACES	1,00	0,00	0,00	1,00
FUENTES DE PODER	0,00	0,00	1,00	1,00
TARJETA DE SERVIDORES	1,00	0,00	0,00	1,00
ENERGIA ELECTRICA	0,00	0,00	1,00	1,00
CIRCUITO ELECTRICO	0,00	0,00	1,00	1,00
VENTILADORES	0,00	0,00	1,00	1,00
CARCASA	1,00	0,00	0,00	1,00
LAZO DE RED	0,00	0,00	1,00	1,00
IOS	1,00	0,00	0,00	1,00
ARCHIVO CONF	1,00	0,00	0,00	1,00
SFP	0,00	1,00	0,00	1,00
FRECUENCIA EVENTOS CONMUTADOR DE NÚCLEO	TOTAL CRITICO	TOTAL MEDIO	TOTAL BAJO	TOTAL
	5,00	1,00	6,00	12,00

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

Gráfico N°14 : Frecuencia de Eventos en Conmutador de Núcleo
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

Cuadro N° 14

NIVELES DE RIESGO EN CONMUTADOR DE ACCESO

DEPENDIENDO DE LA FALLA DEL COMPONENTE CRITICIDAD

CONMUTADOR DE ACCESO	EVENTOS CRITICOS	EVENTOS MEDIOS	EVENTOS BAJOS	FRECUENCIA
FUENTES DE PODER	1,00	0,00	0,00	1,00
TARJETA PRINCIPAL	1,00	0,00	0,00	1,00
ENERGIA ELECTRICA	0,00	0,00	1,00	1,00
LAZO DE RED	0,00	0,00	1,00	1,00
IOS	1,00	0,00	0,00	1,00
ARCHIVO CONF	1,00	0,00	0,00	1,00
SFP	0,00	1,00	0,00	1,00
FRECUENCIA EVENTOS CONMUTADOR DE ACCESO	TOTAL CRITICOS	TOTAL MEDIOS	TOTAL BAJOS	TOTAL
	4,00	1,00	2,00	7,00

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

Gráfico N°15 : Frecuencias de Eventos en Conmutador de Acceso
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

Cuadro N° 15

NIVELES DE RIESGO EN ENRUTADOR DEPENDIENDO DE LA FALLA DEL COMPONENTE

ENRUTADOR	EVENTOS CRITICOS	EVENTOS MEDIOS	EVENTOS BAJOS	FRECUENCIA
TARJETA PRINCIPAL	1,00	0,00	0,00	1,00
ENERGIA ELECTRICA	0,00	0,00	1,00	1,00
IOS	1,00	0,00	0,00	1,00
ARCHIVO CONF	1,00	0,00	0,00	1,00
FRECUENCIA EVENTOS ENRUTADOR	**TOTAL CRITICOS**	**TOTAL MEDIOS**	**TOTAL BAJOS**	**TOTAL**
	3,00	0,00	1,00	4,00

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

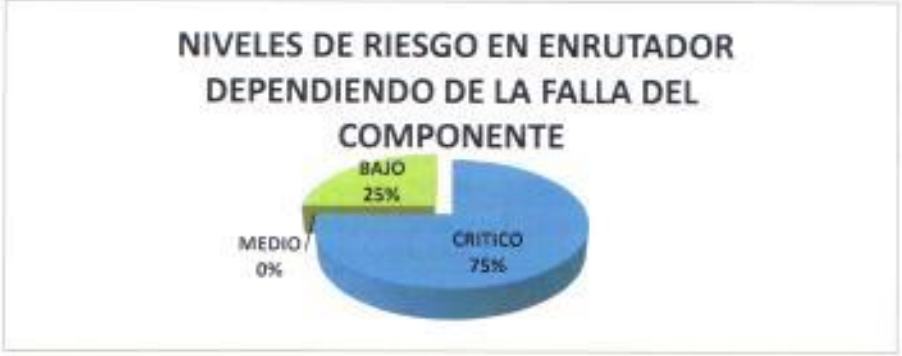


Gráfico N°16 : Frecuencia Eventos Enrutador
Fuente : Investigación
Elaboración : Eduardo Alvarado Unamuno

3.5 Acciones de Contingencias Actuales ante Fallos de Dispositivos de Red.

El siguiente cuadro indica las acciones de contingencias ante las posibles fallas que se puedan presentar en la infraestructura de red.

Cuadro N° 16

Acciones de Contingencia

DISPOSITIVO	FALLO	ACCIÓN DE CONTINGENCIA
Conmutador de Núcleo/Agrega - Cisco 4507R	Tarjeta Procesadora	La falla de una tarjeta procesadora no afecta la operación del equipo ya que cuenta con dos tarjetas procesadoras.
	Tarjeta de Enlaces ascendentes WS-X4506-GB-RJ45	El equipo solo posee una sola tarjeta, el fallo de esta tarjeta dejaría incomunicada, no hay contingencia para esta tarjeta.
	Fuente de poder de 1300W	Se posee dos fuentes de poder, en caso de falla de una La segunda fuente tiene capacidad para soportar toda la carga, no afecta la operación del equipo
	Fallo de Tarjeta WS-X4424-GB-RJ45	El equipo solo posee una tarjeta en caso de falla se perdería conectividad con los servidores. No hay contingencia
	Energía Eléctrica	El hospital posee UPS y Generados
	Circuito Eléctrico	El hospital tiene cada fuente en circuitos independientes.
	Ventiladores	El equipo posee un juego de ventiladores de respaldo.
	Carcasa	Este equipo es de Clase portadora, su matriz de conmutación es pasiva, No hay contingencia.
	Lazo en la red	El equipo tiene configurado esta protección, con la funcionalidad de STP.
	IOS	En caso de falla del IOS del Chasis el equipo se quedaría sin funcionar. No hay contingencia.
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar. No hay contingencia
	Fallos de SFP de los enlaces ascendentes	En caso de falla de un SFP de los enlaces ascendentes sé quedaría un piso sin conectividad con la red. No hay contingencia.
Conmutador de Acceso	Fuente de poder	En caso de fallo de la fuente de poder, se tiene un conmutador de remplazo en sitio Cisco de 24 puertos.
	Lazo en la red	El equipo tiene configurado esta protección con la funcionalidad STP.
	IOS	En caso de falla del IOS en el equipo se quedaría sin funcionar. Se tiene un conmutador de remplazo en sitio Cisco de 24 puertos.
	Tarjeta principal	En caso de fallo de la fuente de poder, se tiene un

		conmutador de remplazo en sitio Cisco de 24 puertos.
	Fallo de SFP de enlaces ascendentes	En caso de falla de un SFP de los enlaces ascendentes se que daria un piso sin conectividad con la red. Se tiene un conmutador de remplazo en sitio Cisco de 24 puertos.
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar. Se tiene un conmutador de remplazo en sitio Cisco de 24 puertos.
	Energia Eléctrica	En caso de falla el hospital posee un UPS y Generador eléctrico.
Fibra Óptica de enlaces ascendentes	Corte	En caso de fallo de la fibra óptica los pisos quedarían incomunicada la red. No hay contingencia
Enrutador 806	Tarjeta Principal	En caso de fallo de la fuente de poder, se tiene un enrutador de remplazo en sitio como contingencia.
	IOS	En caso de falla del IOS en el equipo se quedaría sin funcionar, se tiene un enrutador de remplazo en sitio como contingencia.
	Configuración	En caso de borrado del archivo de configuración el equipo se quedaría sin funcionar. Se tiene un enrutador de remplazo en sitio como contingencia.
	Energia Eléctrica	En caso de falla el hospital posee un UPS y Generador eléctrico.

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

3.6 Análisis Costo Beneficio.

A continuación, en el siguiente cuadro se muestra el análisis costo beneficio para este proyecto.

Se indican las consideraciones para nuestro análisis, este hospital cuenta con 24 consultorios con un promedio de 4 consultas por hora y un costo promedio de $6,00 la consulta, en farmacia se considera 120 recetas vendidas por hora a un valor de $ 20,00 por receta.

la consulta, en farmacia se considera 120 recetas vendidas por hora a un valor de $ 20,00 por receta.

Cuadro N° 17

Análisis costo beneficio

COSTO	Valor	BENEFICIO	Valor /1 Hora	Valor/4 horas	Valor/8 horas	Valor/12 Horas
Conmutador Cisco 2960S	$ 6.496,80	Atención en Consultorios.	$ 576,00	$ 2.304,00	$ 4.608,00	$ 4.608,00
SFP - Conectividad	$ 5.596,00	Atención en Farmacia.	$ 2.400,00	$ 9.600,00	$ 19.200,00	$ 28.800,00
Enrutador Cisco 2911	$ 3.674,40					
Imagen (IOS) Núcleo	$ 300,00					
Sistema de Gestión	$ 9.595,20	Personal Técnico	$ 60,00	$ 240,00	$ 480,00	$ 720,00
Tarjeta Conmutador de Núcleo	$ 4.396,00					
Instalación y Configuracion	$ 3.500,00					
TOTAL	**$ 33.548,40**		**$ 3.036,00**	**$ 12.144,00**	**$ 24.288,00**	**$ 34.128,00**
RAZON (Beneficio/ Costo)			**0,09**	**0,36**	**0,72**	**1,01**

Fuente : Datos de Investigación
Elaboración: Eduardo Alvarado

Análisis: De acuerdo al análisis realizado, se observa que en solo 12 horas teniendo un problema serio en la red se tendría pagado el proyecto, asumiendo que solo se afectaría las áreas de consultorios y farmacia del hospital.

Consideraremos que se paralizan los servicios de atención a los pacientes en consultorios y farmacia del hospital por motivos de cálculo, ya que en la realidad, las labores dentro de estas áreas se realizaran manualmente, la asignación de turnos a los

consultorios, la disponibilidad de las historias clínicas, resultados de los exámenes, etc.

Dado que las labores de estas áreas se realizan manualmente, el primer inconveniente es la disponibilidad de las historias clínicas de los pacientes, ya que al estar todo digitalizado y no tener disponibilidad de la red se dificulta el acceso a los mismos y demandaría más trabajo administrativo retrasando la operación normal de estas áreas.

En la farmacia al no tener los sistemas de facturación y verificación de inventarios de medicina se dificultaría la atención a los usuarios y se realizarían procesos manuales de facturación, una vez restablecidos los sistemas tendrían que ser ingresados al sistema, generando doble trabajo administrativo. No se considera otras áreas como emergencias, hospitalización, etc.

Adicionalmente se indica la criticidad de no poder contabilizar la pérdida de la vida de un paciente por la falta de uno de los servicios antes indicados.

Por lo que se justifica plenamente este proyecto de rediseño de la red que permitirá:

- Mitigar los efectos de los problemas de red por puntos de falla en la misma.
- Reducir las perdidas de desconexión de la red, por daño o fallo e uno de los dispositivos.
- Realizar una gestión proactiva en los dispositivos de red.
- Tener un esquema de red que le permita crecer de manera escalable.

- Permitir a futuro implementar su nuevo sistema Servinte -Hipócrates.
- Implementar a futuro sistemas de Voz sobre Ip, Calidad de Servicio y Multidifusión.
- Implementar a corto plazo Telemedicina.

CAPITULO 4

SERVICIOS A SOPORTAR y REDISEÑO DE INFRAESTRUCTURA LAN Y WAN.

La mayoría de las organizaciones de atención de salud tienen una infraestructura de red existente a menudo tienen varias redes separadas físicamente los datos clínicos, datos no clínicos, voz, investigación y, posiblemente, el equipo educativo y los usuarios. Por varias razones (de gestión, eficiencia, costos, hay un movimiento de convergencia de estas redes separadas para utilizar la misma infraestructura física sin dejar de ofrecer el aislamiento, seguridad y calidad de servicio (QoS) necesaria para las aplicaciones de atención médica.

Algunas definiciones que se usan en la industria del cuidado de la salud son:

Red de Grado Médico - Esta es una red basada en estándares y mejores prácticas en la industria de redes que deliberadamente se aborda las necesidades únicas de una organización de cuidado de la salud. La lista de las necesidades puede parecer bastante universal: La interoperabilidad, seguridad, disponibilidad, productividad y flexibilidad. Sin embargo, estos requisitos son para cumplir una misión fundamental de la organización de salud brindar atención óptima a los pacientes.

Redes Convergentes – Corresponde a implementar todas las redes lógicas de una organización en una infraestructura física común.

Datos clínicos – Son los datos (incluyendo video) desde cualquier dispositivo o equipo relacionados con la atención directa al paciente. Por ejemplo, esto podría ser un monitor de ritmo cardíaco, un monitor de cabecera recogida de signos vitales, una bomba de infusión, o un ventilador. Otros términos para los datos clínicos incluyen información clínica y de sistemas clínicos.

Datos clínicos críticos de la vida - Una clase de Datos para marcar con QoS producido por los dispositivos de red de datos clínicos, que apoyan la vida crítica. Es una red virtual independiente que puede ser utilizado para separar a los dispositivos clínicos críticos de la vida del paciente, de los otros dispositivos de red.

Red de clientes - Incluye todos los pacientes, visitantes y proveedores que tienen conexión a la red de la salud, pero independientes de las computadoras bajo la jurisdicción de la organización.

En el diseño de una infraestructura de red convergente para la LAN en un centro de salud, nos basamos en el tradicional modelo jerárquico de tres capas (núcleo, distribución, acceso). Esta jerarquía establece el marco general y la conectividad para toda la red. Dentro de cada capa existen módulos que sirven a una función específica

en esa capa. Como se requieren cambios o mejoras, se pueden realizar en una sola capa en la jerarquía, sin interrupciones o cambios significativos en las otras capas. Siempre que sea posible, se utiliza enrutamiento de capa 3 de extremo a extremo a través de la red para proporcionar estabilidad de la red y respuesta rápida.

Para implementar la alta disponibilidad en toda la infraestructura de red, por lo general se utiliza el diseño con dispositivos redundantes, especialmente para el núcleo y la capa de distribución. Se observa que un diseño estándar, basado en dispositivos redundantes, es predecible, fácil de implementar, escalable, y relativamente fácil de mantener.

4.1 Servicios de Software

4.1.1 Imágenes Médicas

La infraestructura que soporte imágenes médicas, se deben basar en tecnologías que proporcionan una infraestructura altamente disponible y escalable para soportar las Imágenes Archivo de Sistema de Comunicación (PACS) que se utiliza hoy en día en la medicina.

A través de una red de grado medico, se ofrece una red escalable de imágenes y se aumenta el rendimiento de los PACS y permiten gestionar hoy en día grandes anchos de banda para soportar las imágenes. Son compatibles con el almacenamiento

centralizado de imágenes para acceder a las imágenes rápidamente y la recuperación a través de una distribución entorno de almacenamiento.

Las aplicaciones de estos productos se producen a través de consultas directas con las áreas de radiología o de imágenes para hacer frente a muchos problemas clave como el crecimiento y la complejidad de los servicios de imagineología que aumentan de forma exponencial.

A continuación se adjunta en el cuadro 14 estadísticas de volúmenes de tráfico esperados en un hospital.

4.1.2 Software Hipócrates (HIS).

HIPOCRATES es un sistema de información integrado que maneja de una manera ágil, integrada y eficiente todos los procesos médico-administrativos de las instituciones prestadoras de servicios de salud, haciendo énfasis en una mejor atención al paciente así como en la gestión interna de la institución.

Principales características:

- Es una solución diseñada especialmente para el sector salud.
- Alcance global: procesos de atención a pacientes, procesos administrativos, procesos financieros, contables y de gestión.

Cuadro N° 18

Volumen de tráfico esperado en un hospital

# of Scanners	Modality	Matrix			Bits Stored	Image Capture	MB/ Image	Images/ Exam	MB/ Exam	Exams/ Year	Exam/ Day	Images/ Day	MB/ Day	MB/ Year
	DSA	1,024	X	1,024	16	DICOM	2		0		0	0	0	0
1	NUCLEAR	256	X	256	24	DICOM	0	70	2	5,000	6	427	35	5,288
2	ULTRASOUND (256)	512	X	512	16	DICOM	1	38	[illegible]	7,000	16	575	302	110,208
	ULTRASOUND (256)	512	X	512	16	DICOM	1		0		0	0	0	0
1	CT - Standard	512	X	512	16	DICOM	1	60	31	6,000	22	1,318	688	251,458
1	MRI	256	X	256	16	DICOM	0	160	21	10,000	27	4,342	575	209,715
	Digitizer	2,048	X	2,560	16	DICOM	10		0		0	0	0	0
3	Comp. Rad (CR)	2,048	X	2,560	16	DICOM	10	3	20	67,000	178	445	4,088	1,720,838
1	CT 16-Slice	512	X	512	16	DICOM	1	200	105	4,000	11	2,192	1,148	438,480
	CT 64-Slice	512	X	512	16	DICOM	1		0		0	0	0	0
	XA	512	X	512	16	DICOM	1		0		0	0	0	0
	MRI	512	X	512	16	DICOM	1		0		0	0	0	0
	Digital Mammo	1,000	X	5,024	16	DICOM	10		0		0	0	0	0
	Cath Lab	1,024	X	1,024	16	DICOM	2		0		0	0	0	0
1	Special Procedures	1,024	X	1,024	16	DICOM	2	8	51	1,000	3	41	35	21,457
1	Echo	512	X	512	16	DICOM	1	150	64	2,400	9	712	373	136,315
11										109,900	274	4,727	7,419	2,888,321

Fuente : Cisco Systems
Elaboración: Cisco Systems

- Totalmente parametrizable.
- Más de 15 años de experiencia en el mercado.
- Modular: se puede instalar e implementar por fases.
- Actualización permanente de acuerdo a los cambios del legislación del sector.
- Orientada a costos: permite conocer costos por centro de costo y por actividad.
- Mejora la calidad y la oportunidad de la información, sin necesidad de duplicación de esfuerzos operativos o administrativos.

- Maneja información a nivel operativo y gerencial.

Algunos módulos del sistema Hipócrates son:

Admisiones	Caja y Bancos
Facturación	Cuentas por pagar
Ayudas diagnósticas	Liquidación de terceros
Citas	Activos Fijos
Cirugía	Contabilidad
Laboratorio Clínico	Nómina
Cuentas por cobrar	Costos
Suministro, Inventario y Farmacia	Administración de documentos
Contabilidad	Presupuesto
	Sistema de Información Gerencial

De forma general de lo expuesto anteriormente los servicios a prestar en esta red son:

- Servicios de transmisión de datos (Hipócrates, Internet, Ofimática)
- Servicios de Telefonía IP (a futuro).
- Imágenes de grado medico (a futuro).
- Sistemas de Datos críticos de la vida (a futuro).

4.2 Rediseño de la Nueva Arquitectura de Red.

4.2.1 Rediseño de la Red LAN

4.2.1.1 Capacidad de Enlaces Ascendentes.

Las consideraciones de diseño se enfocarán a concebir una red integrada que sirva como medio de comunicación a través del cual circulen eficientemente los flujos de voz, datos y video asegurando la implementación a futuro de calidad de servicio (QoS) y disponibilidad sobre dicho medio, lo cual, permitir facilitar las tareas diarias de los funcionarios del hospital.

En el Gráfico 15 se adjunta la nueva arquitectura de red LAN, en el rediseño de la nueva arquitectura de red se reutilizara el conmutador de núcleo.

Se adjunta tráfico actual correspondiente a los pisos de Laboratorio, Consulta Externa, Hospitalización Este y Administración respectivamente.

Gráfico N°17

Tráfico de red en enlaces ascendentes

Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

A continuación se detalla dicho tráfico para determinar la capacidad de los enlaces ascendentes hacia las distintas áreas.

Cuadro N° 19

Tráfico de Red Actual en Enlaces Ascendentes

PISO	TRÁFICO ENTRANTE		TRÁFICO SALIENTE	
	Mbps (max)	Mbps (Promedio)	Mbps (max)	Mbps (Promedio)
LABORATORIO	2,290	0,078	4,538	0,320
CONSULTA EXTERNA	6,254	0,176	4,053	0,284
HOSPITALIZACIÓN ESTE	2,735	0,168	13,623	0,917
ADMINISTRACIÓN	3,867	0,104	5,843	0,643
Promedio	**3,7865**	**0,1315**	**7,01425**	**0,541**

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

Actualmente en la red, en los enlaces ascendentes se tiene un tráfico promedio general entrante de aproximado de 0,14 Mbps y saliente 0,55 Mbps, con picos en aproximadamente 3,8 Mbps entrante y 7 Mbps salientes, con lo que con una interfaz de 1 Gbps esta muy holgada para el trafico actual.

Si tomamos el valor total del tamaño de archivos de imágenes que se producen por día, del cuadro 11 es 7859 MB los cuales traducidos a Giga bits es 61,39Gbxdia los cuales en promedio por hora 2,55 Gb x hora, el cual llevado a Gbps es 0,0071 o sea 7.1 Mbps con lo que el trafico total incluido exámenes e imágenes seria de 8.1 Mbps promedio, lo cual se considera muy buen desempeño considerando que se tendrá un

ancho de banda de 2Gbps y un 1 Gbps en el caso de que uno de los enlaces ascendentes falle.

4.2.1.2 Diseño de la Alta Disponibilidad de la Red LAN.

El equipo 4507R soporta alta disponibilidad en supervisora y fuentes de poder, el equipo actualmente cuenta con dos tarjetas supervisoras por lo que se mantendrá con las mismas supervisoras, los cuales les da una capacidad de 64 Gbps, funcionando en activo/pasivo.

Se agrega una tarjeta WS-X4506-GB-, permitiendo incrementar un enlace de 1Gbps por piso y configurar ether canales, para tener un enlace troncal de 2 Gbps. Dado que estas tarjetas se conectan a la matriz de conmutación del equipo a 6Gbps no existe sobre subscripción en los enlaces de conexión del acceso al núcleo/agregación.

Al agregar esta tercera tarjeta WS-X4506GB la capacidad de la fuente del conmutador de 1300W esta al 51% por lo que esta garantizada la redundancia en la fuente de poder.

En esta topología el conmutador de núcleo realizara también la función de agregación del tráfico de los conmutadores de acceso, la misma que será realizada con las tarjetas WS-X4506-GB.

Se remplaza el conmutador 3COM por un conmutador Cisco WS-C2960S, adicionalmente en los pisos que se tiene dos conmutadores se realizara la interconexión por los puertos de enlaces ascendentes, igualmente se agregara un segundo enlace para subir el ancho de banda de la conexión de los dos conmutadores a 2 Gbps formando un Ether canal.

Se alojara otra tarjeta WS-X4424-GB-RJ45 en el cisco Catalyst 4500 para la alta disponibilidad en los servidores, se formara ether canales con soporte de IEEE 802.3ad (LACP) que también soportan los servidores del hospital.

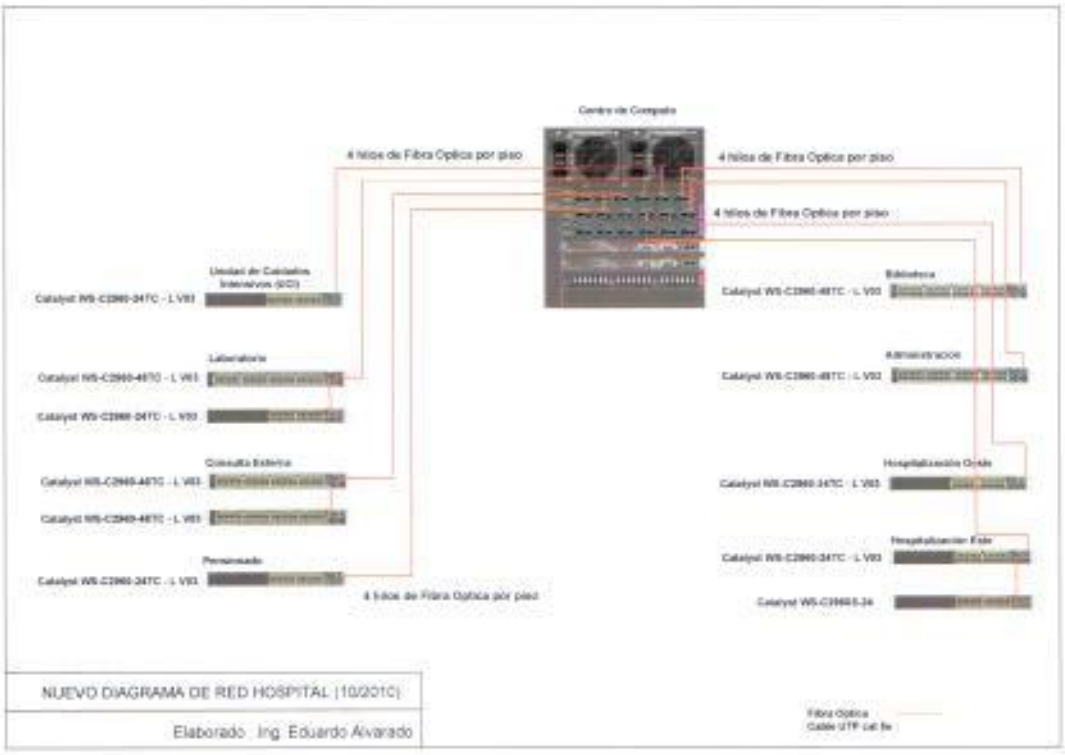


Gráfico N°18 : Nuevo Diagrama de Red LAN
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

4.2.1.3 Funcionalidades a ser Soportadas por los Dispositivos de Red LAN.

Para aislar el tráfico de las distintas áreas se procederá a implementar redes virtuales, se asignara una red virtual por cada conmutador o grupo de conmutadores de acceso. Adicionalmente se debe configurar el enrutamiento entre redes virtuales en los puertos de las tarjetas WS-X4506-GB, dado que el conmutador Cisco 4507R cumple la función de núcleo/agregación no es necesario implementar un protocolo de enrutamiento dinámico.

Se procede a detallar las nuevas funcionalidades a configurar en los conmutadores de núcleo y acceso para soportar redundancia y la alta disponibilidad.

Cuadro N° 20

Funcionalidades a Configurar en Conmutadores de Núcleo y Acceso

FUNCIONALIDADES REQUERIDAS	FUNCIÓN DEL CONMUTADOR
Vlan´s	Núcleo
Inter Vlan´s routing.	Núcleo
VTP server	Núcleo
Etherchannel – LACP	Núcleo
PVSTP+	Núcleo
Redundancia (Supervisora)	Núcleo
Redundancia (Power Supplies)	Núcleo
RootGuard	Núcleo

FUNCIONALIDADES REQUERIDAS	FUNCIÓN DEL CONMUTADOR
Vlan´s	Acceso
PortFast	Acceso
VTP client	Acceso
Etherchannel – LACP	Acceso
PVSTP+	Acceso
LoopGuard	Acceso

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

Adicionalmente el conmutador tenía un sistema operativo IP-Base, pero para dar soporte a las funcionalidades requeridas se remplaza por una imagen empresarial.

4.2.2 Rediseño de la Red WAN

4.2.2.1 Diseño de Alta Disponibilidad de WAN.

Para el esquema de alta disponibilidad en la conectividad WAN se presenta el siguiente diagrama, durante este diseño se considera dar alta disponibilidad al anillo de formado por los enlaces de radio. A futuro se implementara el esquema de alta disponibilidad en las puertas de enlace de cada LAN, con alguno de los protocolos utilizados tales como GLBP, HSRP o VRRP.

Dado que inicialmente este es una red en capa 2 se eliminan los conmutadores que estaban colocados después de los enrutadores y se utiliza para los enrutadores que forman el anillo de tres interfaces LAN ruteadas. El protocolo de enrutamiento elegido es OSPF por su rápida convergencia y alta escalabilidad, considerando que es

un protocolo estándar. En la caso de integración con otras redes será muy útil que sea un protocolo estándar y no uno propietario. El mismo tiene como métrica el ancho de banda.

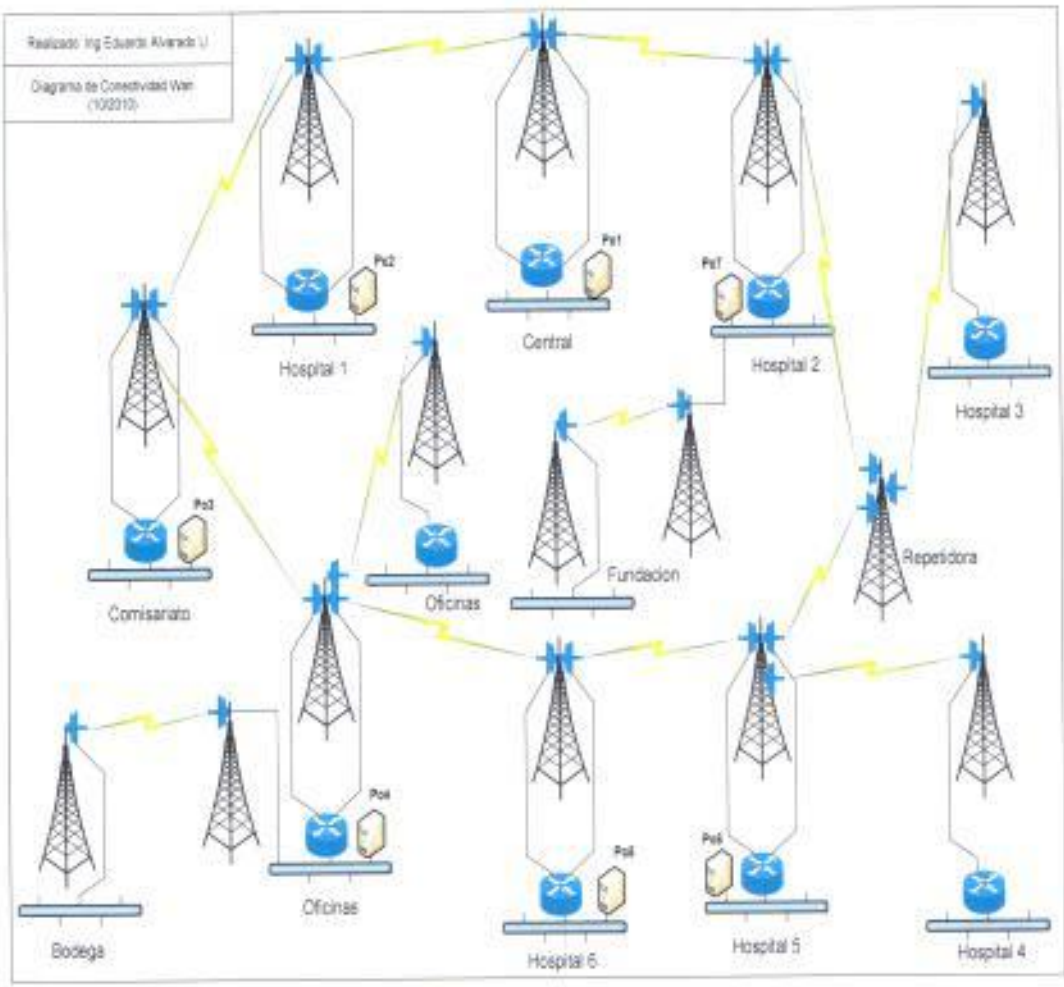


Gráfico N°19 : Nuevo Diagrama de Red WAN
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Dada la arquitectura de la red y la no disponibilidad de cambiar la topología de la red WAN, ya que son enlaces de radio por el momento se implementara a todos los dispositivos en una sola área, el área 0.

A continuación se indica el tráfico de WAN:

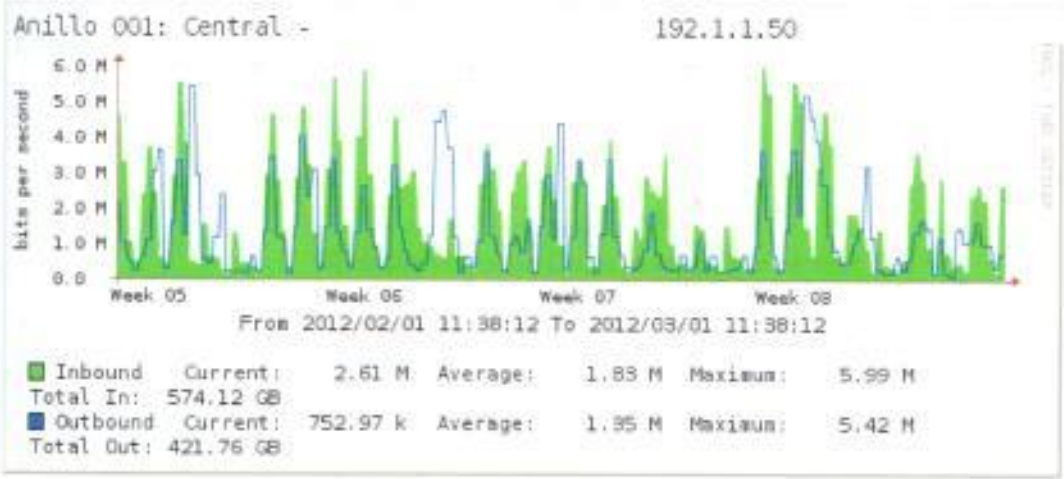


Gráfico N°20 : Trafico WAN actual
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Actualmente el trafico promedio de los enlaces WAN 1,83 Mbps pero con máximos de 6 Mbps, la grafica corresponde al punto donde se interconectan todos los hospitales con la oficina central es decir representa el punto de mayor trafico.

El anillo de interconexión de la WAN soporta una velocidad máxima de 10 Mbps. Es decir se encuentra al aproximadamente al 60% en su momento, de acuerdo a la tabla de Rendimiento de enrutadores de Cisco los enrutadores 2600 y 2800 ya se encuentran en fin de venta por lo que los modelos a elegir son de los modelos ISR G2 con procesadoras de video (DSP) incluidos, particular que los hace ideales para esta implementación.

Se elige el modelo ISR G2 2911 ya que este modelo permite colocar Network Módulos y a futuro permitiría implementar soluciones de optimizadores de ancho de banda y aceleradores de aplicaciones. La imagen a elegir es IP Base ya que esta soporta OSPF.

Cuadro N° 21
Rendimiento de Enrutadores Cisco ISR G2

Platform	Process Switching		Fast/CEF Switching		EOS?
	PPS	Mbps	PPS	Mbps	
262X	1,500	0.768	25,000	12.80	26-Apr-03
265X	2,000	1.024	37,000	18.94	26-Apr-03
261X(XM)	1,500	0.768	20,000	10.24	27-Mar-07
262X(XM)	1,500	0.768	30,000	15.36	27-Mar-07
265X(XM)	2,000	1.024	40,000	20.48	27-Mar-07
2691	7,400	3.7888	70,000	35.84	27-Mar-07
ISR 2801	3,000	1.536	90,000	46.08	No
ISR 2811	3,000	1.536	120,000	61.44	No
ISR 2821	11,500	5.888	170,000	87.04	No
ISR 2951	15,000	7.68	220,000	112.64	No
3620	2,000	1.024	20,000 – 40,000	10 - 20	31-Dec-03
ISR G2 2901			327,000	167.42	No
ISR G2 2911			353,000	180.73	No
ISR G2 2921			480,000	245.76	No
ISR G2 2951			580,000	296.96	No

Fuente : Cisco Systems (http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf
Elaboración : Cisco Systems

4.2.2.2 Funcionalidades a ser Soportadas por los Dispositivos de Red WAN.

Las funcionalidades requeridas en los enrutadores son las indicadas en el cuadro N° 18, se solicita la opción de multidifusión para el manejo eficiente del video, se

solicitan 3 interfaces ruteadas ya que dos se utilizan para realizar el anillo y la tercera es para la LAN interna de cada sitio.

Cuadro N° 22
Funcionalidades en Enrutadores

FUNCIONALIDADES REQUERIDAS ACTUALES	**CAPACIDAD**
OSPF	Si
Interfaces Ruteadas	3
Capacidad de envió	180 Mbps
Multidifusión	Si
Velocidad de Interfaces	1 Gbps
FUNCIONALIDADES REQUERIDAS A FUTURO*	**CAPACIDAD**
Soporte de Ipsec	Si
Soporte de VPN	Si
Soporte de IOS IPS	Si
Soporte de IOS Firewall	Si

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

Nota*: En una segunda fase, que será implementada a futuro por el cliente, se revisara los aspectos de seguridad de la red. Dado esto se indica que los enrutadores Cisco 2900 ISR2 soportan las características solicitadas, con solo la activación de la licencia de seguridad y se tiene la ventaja también de activar un demo de la licencias por 60 días.

4.3 Selección del Software de Monitoreo y Gestión de los Dispositivos de la Red.

Las redes y los sistemas de procesamiento distribuido son de una importancia crítica y creciente en los negocios, gobierno y otras instituciones. Dentro de una institución, la tendencia es hacia redes más grandes, más complejas y dando soporte a más aplicaciones y a más usuarios.

Una red grande no se puede instalar y gestionar sólo con el esfuerzo humano. La complejidad de un sistema tal, impone el uso de herramientas automáticas de gestión de red. La urgencia de la necesidad de esas herramientas se incrementa, y también está en auge la dificultad de suministrar dichas herramientas, si la red incluye equipos de múltiples distribuidores. En respuesta, se han desarrollado normalizaciones para tratar la gestión de red, y que cubren los servicios, los protocolos y la base de información de gestión.

4.3.1 Requerimientos para la Gestión y Monitoreo de la Red.

Los requerimientos del departamento de sistemas, es un sistema de monitoreo y gestión para de forma permanentemente y proactiva monitorear y gestionar la salud de la red y no trabajar de una manera solo reactiva, el software debe tener las siguientes funcionalidades:

- Agendar el respaldo automático de los archivos de configuración Cisco.

- Agendar el respaldo automático de las imágenes IOS de los equipos Cisco.
- Soporte de protocolo SNMP.
- Colección de eventos estadísticos.
- Actualización de imágenes IOS en forma remota.
- Envió de alarmas vía correo electrónico.
- Permita realizar el inventario de los dispositivos de red al detalle de chasis, modulo e interface.
- Monitoreo del performance de los equipos.
- Analizador de protocolo integrado en la herramienta.
- Facilidad en acceso a soporte y documentación de la herramienta.
- Auto descubrimiento de la red.

Permitiendo la recolección, almacenamiento de históricos y análisis de las principales variables de la red (Memoria, consumo de CPU, consumo de memoria RAM, tráfico de las interfaces, etc.), además de permitir monitorear permanentemente los retardos de los enlaces WAN parámetro que es de gran utilidad especialmente para las aplicaciones de voz, también nos brinda una visión de la disponibilidad de la red.

Adicionalmente resulta de gran utilidad contar con la herramienta de análisis de protocolos, y a través de la configuración de puertos espejos en los conmutadores administrables permite conocer cualitativamente el tráfico que esta fluyendo a través de la red, de este modo se puede diagnosticar de mejor manera los problemas que pueden surgir, así como también permite identificar tráfico indeseable o utilidades de

internet que no son productivas para el desarrollo del trabajo hospitalario y más bien producen un consumo innecesario de ancho de banda.

4.3.2 Análisis y Selección de Software de Monitoreo y Gestión.

A continuación se describe tres software de gestión y monitoreo, dos de código abierto y una del fabricante de los equipos de la red LAN y WAN.

CACTI, es una herramienta que permite monitorizar y visualizar gráficas y estadísticas de dispositivos conectados a una red y que tengan habilitado el protocolo SNMP. En determinados momentos, necesitamos visualizar gráficas del estado de nuestra red: ancho de banda consumido, detectar congestiones o picos de tráfico o monitorizar determinados puertos de un equipo de red.

Con Cacti podremos monitorizar cualquier equipo de red que soporte el protocolo SNMP, ya sea un conmutador, un enrutador o un servidor Linux. Siempre que tengan activado el protocolo SNMP y conozcamos las MIBs con los distintos identificadores de objeto (OID), que podemos monitorizar y visualizar, podremos programar la colección de gráficas con las que queramos realizar el seguimiento. Cacti es una aplicación que funciona bajo entornos Apache + PHP + MySQL, por tanto, permite una visualización y gestión de la herramienta a través del navegador web. La herramienta utiliza RRDtool, que captura los datos y los almacena en una base de

datos circular, permitiendo visualizar de forma gráfica los datos capturados mediante MRTG.

PANDORA FMS, es una herramienta de software libre que permite analizar de forma visual, utilizando un navegador, el rendimiento y estado de algunos parámetros de diferentes Sistemas Operativos, servidores, aplicaciones y sistemas hardware tales como Cortafuegos, Bases de Datos, Servidores Web o Enrutadores.

Hoy en día existe en el mundo una gran preocupación por contar con redes corporativas de telecomunicaciones con la mayor disponibilidad posible, ya que están cada día más fuertemente ligadas a los resultados comerciales que se obtienen.

La importancia que cobra esta necesidad conduce a la búsqueda de alternativas para manejar adecuadamente la información de los equipos en tiempo real y las notificaciones de falla para ofrecer mejores tiempos de respuesta, en materia de resolución de incidencias.

Pandora FMS (Sistema de Monitoreo libre) nace de una serie de necesidades reales y se ha consolidado con el tiempo como una herramienta de monitorización versátil a la vez que robusta, comprometida con el software libre.

Esta adaptabilidad es el principal valor diferenciador de Pandora FMS y ha conseguido posicionar la herramienta en el mercado de una manera estable dando servicio a un gran número de organizaciones.

Algunas de las características principales de Pandora FMS son:

- Monitorización multiplataforma, Solaris, GNU/Linux, Windows, IPSO, AIX, HP-UX.
- Adaptabilidad total, servicios, aplicaciones, puertos, procesos, ficheros log u otra fuente de información.
- Monitorización remota.
- Gestión y lanzamiento de alertas adaptables.
- Generación de informes personalizada.
- Gestión Web.
- Arquitectura Cliente-Servidor.
- Alta capacidad de procesamiento

Cisco LMS, se ha desarrollado de una colección de productos individuales en un conjunto de funciones de gestión integrada basada en la manera que los administradores de red realizan su trabajo. Organizar el producto basado en la función de gestión, simplifica la experiencia del usuario al reducir la necesidad de cruzar los límites de una aplicación para completar una tarea específica de gestión. Los flujos de

trabajo son autónomos y toda la funcionalidad requerida se mantiene dentro de un área funcional.

Se indica las principales áreas funcionales.

- Forma rápida y proactiva para identificar y corregir problemas en la red antes de que afecten a los usuarios finales o servicios.
- Navegador centralizado de fallos y de eventos (consolidado, syslog, trampas, los eventos y alarmas).
- Integración con el Módulo de Análisis de Redes (NAM) para el análisis detallado del rendimiento y resolución de problemas (a nivel de decodificación de paquetes, análisis de protocolos).
- Copia de seguridad de configuración, gestión de imagen de software, el cumplimiento y gestión del cambio necesaria para mantener y actualizar los dispositivos de red.
- Las mejores prácticas de plantillas de configuración para desplegar configuraciones totales o parciales basadas en recomendaciones de diseño validadas.
- Los flujos de trabajo dinámicos dirigidos a reducir las probabilidades de error en las plantillas de configuración, las nuevas actualizaciones y configuraciones se puede descargar fácilmente desde Cisco.com
- Inventario completo y detallado de todos el equipamiento de Cisco chasis, módulo, interfaz.

- Ofrece un único menú del estado del dispositivo.
- Soporte para más de 560 tipos de dispositivos de Cisco.
- Todos los informes están centralizados en un solo menú, lo que simplifica la navegación y el acceso a los informes detallados y la información.
- Todas las funciones administrativas para la instalación y configuración de la aplicación están centralizadas para facilitar el acceso.

A continuación se detalla una tabla de evaluación de los tres software de gestión y monitoreo. Para ello se utilizo el cumplimiento de los aspectos más importantes para el área de IT del Hospital.

CUADRO N° 23

Cuadro de evaluación de funcionalidades de software de gestión y monitoreo

FUNCIONALIDAD	PUNTAJE	PANDORA	CACTI	CISCO LMS
Respaldo Archivos de Configuración	10	0	10	10
Respaldo de Imágenes IOS	10	0	0	10
Actualización de Imágenes en Forma Remota	10	0	0	10
Auto Descubrimiento de la Red	5	5	5	5
Soporte de SNMP	5	5	5	5
Colección de eventos y estadísticas de la Red	5	5	5	5
Envió de alarmas vía correo electrónico	5	5	5	5
Inventario de dispositivos al detalle	5	5	5	5
Monitoreo del Rendimiento de Dispositivos	5	5	5	5
Analizador de Protocolos	5	0	0	5

Interfaz del Usuario Intuitiva	9	9	9	7
Facilidad de acceso a Soporte	8	5	5	8
Facilidad de acceso a Documentación en Línea	8	5	5	8
Costo Licenciamiento (Sin Costo 5 - Con Costo 0)	5	0	5	0
Soporte Virtualización	5	5	5	5
TOTAL	100	54	69	93

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

El software elegido para esta implementación es Cisco LMS 4.0, dado que es mejor contar con una herramienta que nativamente gestione y se integre de mejor manera con los dispositivos de red.

4.4 Pruebas de Simulación WAN

La simulación de la Red WAN de alta disponibilidad fue realizada utilizando el software packet tracer, el diagrama propuesto fue el siguiente:

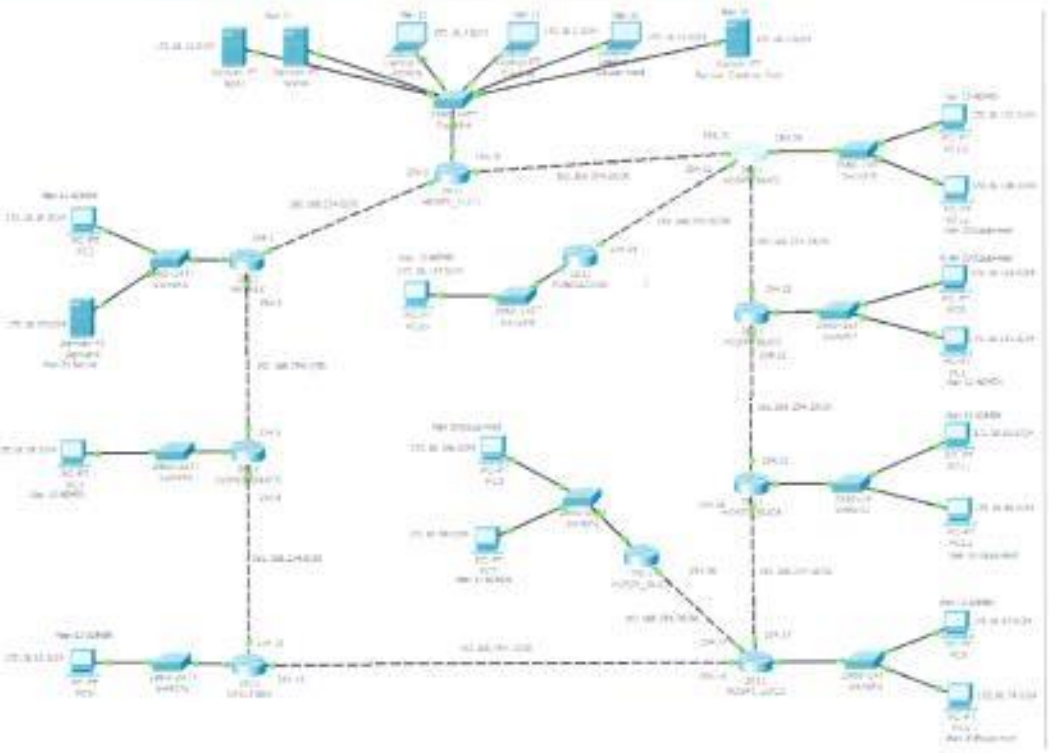


Gráfico N°21 : Diagrama de simulación de la WAN
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Para el diseño WAN de alta disponibilidad se implemento el protocolo de enrutamiento OSPF.

La imagen de los enrutadores es *c2800nm-advipservicesk9-mz.124-15.T1.bin*

```
HOSPI_MATRIZ>ena
HOSPI_MATRIZ#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T
1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

ROM: System Bootstrap, Version 12.1 3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on
System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

Gráfico N°22 : Versión de la Imagen de los enrutadores de simulación
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

A continuación se detalla la configuración de uno de los enrutadores:

```
HOSPI_SUC1#show runn
Building configuration...

Current configuration : 1213 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname HOSPI_SUC1
!
interface Loopback0
 ip address 10.10.10.11 255.255.255.255
!
interface FastEthernet0/0
 bandwidth 10000
 ip address 192.168.254.2 255.255.255.252
 duplex auto
 speed auto
```

```
!
interface FastEthernet0/1
 ip address 192.168.254.30 255.255.255.252
 duplex auto
 speed auto
!
interface Ethernet0/3/0
 no ip address
 duplex auto
 speed auto
!
interface Ethernet0/3/0.1
 encapsulation dot1Q 13
 ip address 172.18.4.1 255.255.255.0
!
interface Ethernet0/3/0.2
 encapsulation dot1Q 11
 ip address 172.18.2.1 255.255.255.0
!
interface Ethernet0/3/0.3
 encapsulation dot1Q 10
 ip address 172.18.1.1 255.255.255.0
!
interface Ethernet0/3/0.4
 encapsulation dot1Q 20
 ip address 172.18.11.1 255.255.255.0
!
interface Ethernet0/3/0.5
 encapsulation dot1Q 21
 ip address 172.18.12.1 255.255.255.0
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 network 192.168.254.0 0.0.0.255 area 0
 network 172.18.0.0 0.0.255.255 area 0
!
ip classless
!
no cdp run
!
line con 0
line vty 0 4
 login
!
end
```

Se detallan las pruebas realizadas:

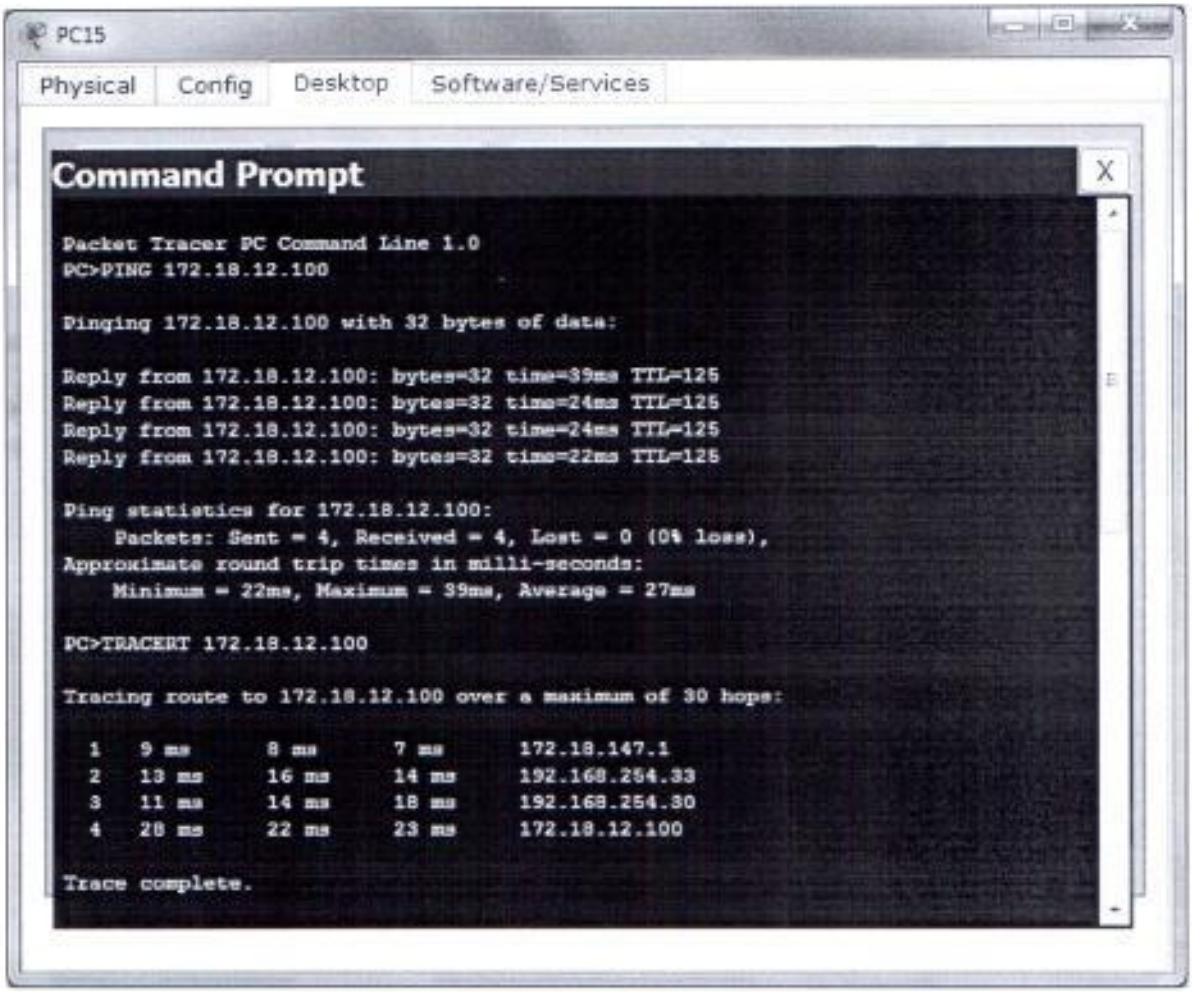


Gráfico N°23 : Pruebas de conectividad de la WAN (Ping-ICMP)
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

En la grafica se demuestra la conectividad entre el Pc15 (172.18.47.100) ubicado en Fundación y un servidor WWW (172.18.12.100) ubicado en la Vlan de 21 en el Hospital 1. Adicionalmente se presente la salida del comando tracert donde se indica que para ir del enrutador Fundación a Hospital 1 se elige la ruta mas cercana para ir al servidor.

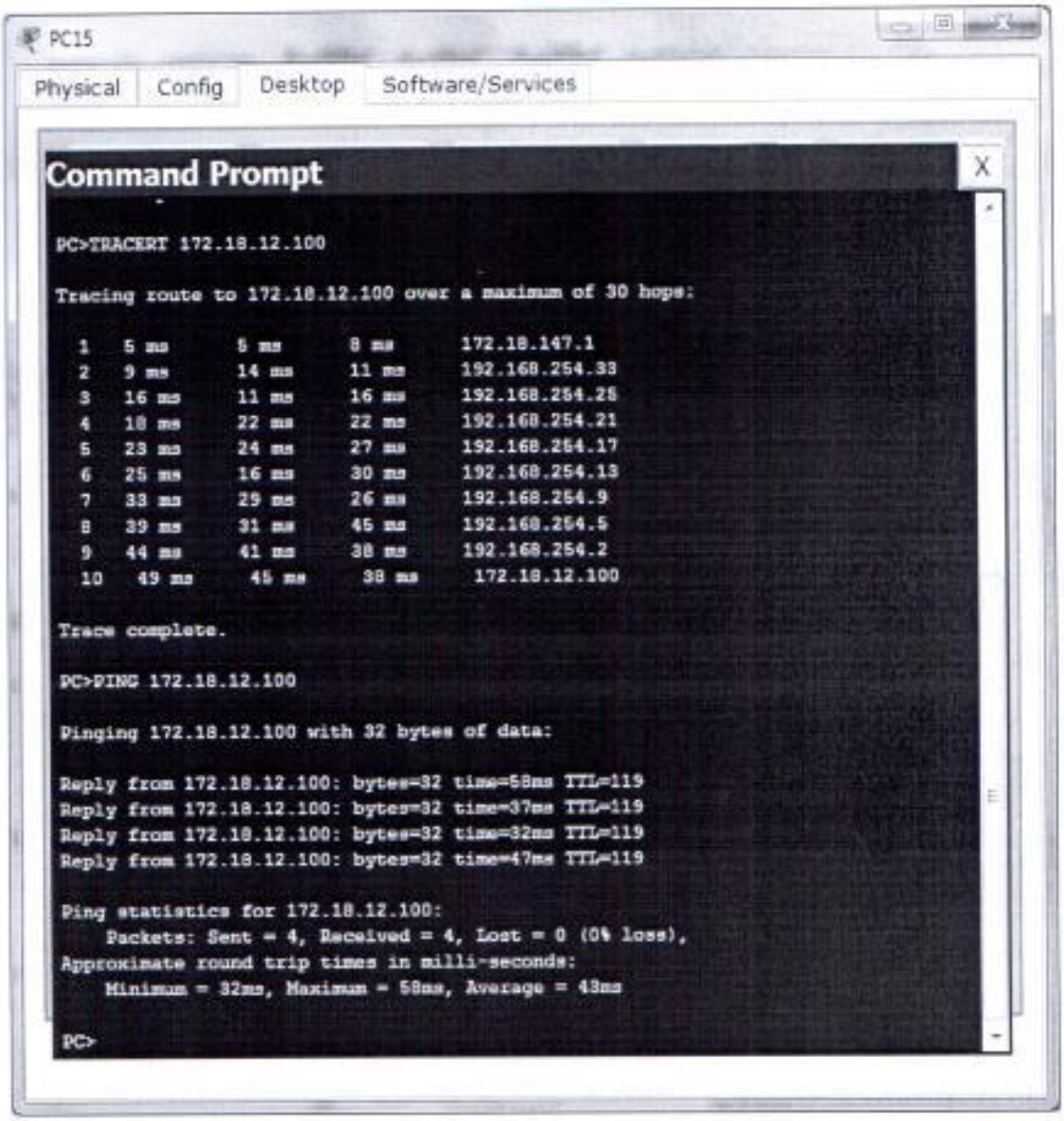


Gráfico N°24 : Pruebas de conectividad de la WAN (Tracer-ICMP)
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

En las graficas 21, 22 y 23 corresponden a una falla producida en el enlace entre HOSPI-SUC1 Y HOSPI_SUC2 ante lo cual se produce un cambio de rutas demostradas con el comando tracer (grafica superior). Donde se aprecia claramente que ahora para ambos destinos se elige la ruta inferior.

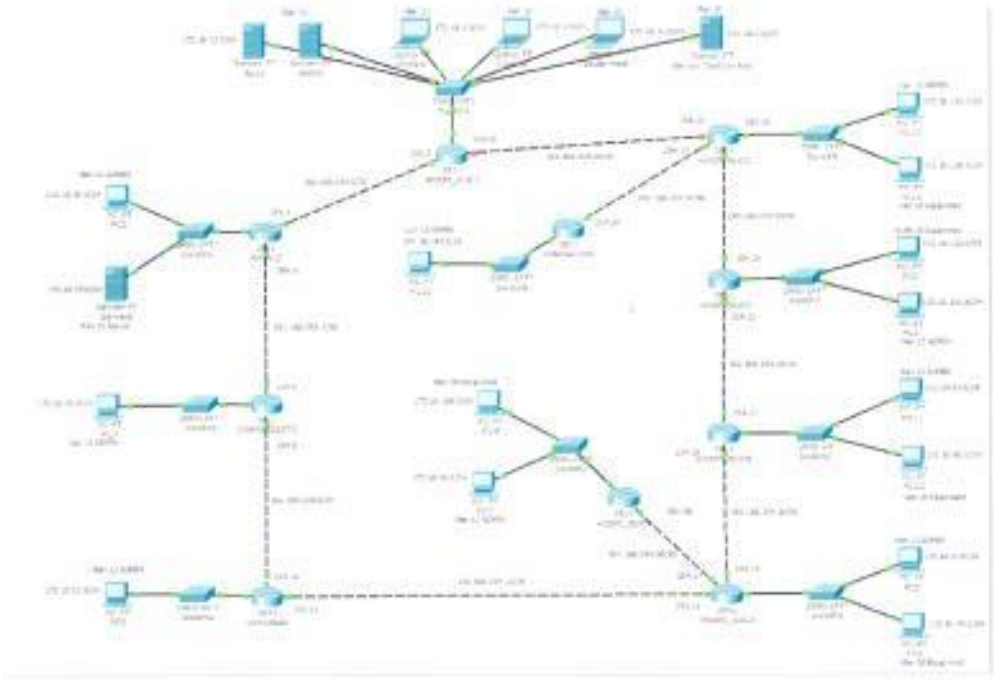


Gráfico N°25 : Gráfico de la WAN donde se observa la falla del enlace.
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Gráfico N°26 : Salida del comando Tracert donde se observa nueva ruta.
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

4.5 Equipamiento Requerido.

A continuación se detallan los nuevos equipos a adquirir:

Cuadro N° 24

Costo del Proyecto de Implementación LAN y WAN

Número Parte	Vendor	Descripción	Precio Unit.	Cantidad	Precio Total
CWLMS-4.0-100-K9	Cisco	LMS 4.0 100 Device Restricted, WIN only	7996,00	1	7996,00
CON-CSSPS-LMS4100	Cisco	SHARED SUPP SAS LMS 4.0 100 Device Device Restricted	1599,20	1	1599,20
				SUBTOTAL SOFTWARE DE GESTIÓN	**9595,20**
WS-C2960S-24TS-L	Cisco	Catalyst 2960S 24 GigE, 4 x SFP LAN Base	2396,00	1	2396,00
GLC-SX-MM=	Cisco	GE SFP, LC connector SX transceiver	400,00	10	4000,00
CAB-16AWG-AC	Cisco	AC Power cord, 16AWG	0,00	1	0,00
CAB-CONSOLE-USB	Cisco	Console Cable 6 ft with USB Type A and mini-B	24,00	1	24,00
CON-CSSPP-2960S2TS	Cisco	SHARED SUPP 24X7X4 Cat 2960S Stk 24 GigE,4xSFP LAN Base	76,80	1	76,80
				SUBTOTAL CONMUTADOR DE ACCESO	**6496,80**
S45IPBK9-12254SG=	Cisco	Cisco CAT4500 IOS IP BASE SSH	300,00	1	300,00
				SUBTOTAL IOS CONMUTADOR DE NÚCLEO	**300,00**
CISCO2911/K9	Cisco	Cisco 2911 w/3 GE,4 EHWIC,2 DSP,1 SM,256MB CF,512MB DRAM,IPB	2156,00	1	2156,00
SL-29-IPB-K9	Cisco	IP Base License for Cisco 2901-2951	0,00	1	0,00
PWR-2911-AC	Cisco	Cisco 2911 AC Power Supply	0,00	1	0,00
ISR-CCP-EXP	Cisco	Cisco Config Pro Express on Router Flash	0,00	1	0,00
MEM-2900-512MB-DEF	Cisco	512MB DRAM for Cisco 2901-2921 ISR (Default)	0,00	1	0,00
MEM-CF-256MB	Cisco	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	0,00	1	0,00
CAB-AC	Cisco	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	0,00	1	0,00
CAB-CONSOLE-USB	Cisco	Console Cable 6 ft with USB Type A and mini-B	24,00	1	24,00
S29UK9-15001M	Cisco	Cisco 2901-2921 IOS UNIVERSAL	0,00	1	0,00
HWIC-1FE	Cisco	1-port 10/100 Routed Port HWIC	720,00	1	720,00
CON-CSSPP-	Cisco	SHARED SUPP 24X7X4 Cisco 2911 w/3 GE,4	774,40	1	774,40

2911					
				SUBTOTAL ENRUTADOR	**3674,40**
WS-X4306-GB=	Cisco	Catalyst 4500 Gigabit Ethernet Module, 6-Ports(GBIC) (Spare)	2396,00	1	2396,00
WS-G5484=	Cisco	1000BASE-SX Short Wavelength GBIC (Multimode only)	400,00	8	3200,00
				SUBTOTAL TARJETA DE CONMUTADOR DE NÚCLEO	**5.596,00**
WS-X4548-GB-RJ45=	Cisco	Catalyst 4500 Enhanced 48-Port 10/100/1000 Base-T (RJ-45)	4396,00	1	4396,00
				SUBTOTAL TARJETA DE CONMUTADOR DE NÚCLEO	**4.396,00**
Servicios Inst.-Conf.	Local	Servicios de Instalación y Configuración	3500,00	1	3500,00
				TOTAL	**33.548,40**

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

4.6 Plan de Implementación de la Solución.

A continuación se presenta el plan de implementación de esta solución:

Cuadro N° 25

Cuadro Detalle del Plan de Implementación LAN, WAN y Monitoreo

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

También se adjunta el diagrama de Gant como Anexo 1.

4.6.1 Plan de Implementación de la Red LAN.

4.6.1.1 Instalación y Configuración de Conmutadores de Acceso.

- Revisión de Infraestructura donde se instalara los equipos (Energía Eléctrica y Aire Acondicionado) para verificación de parámetros recomendados por el fabricante para la instalación de los equipos.
- Instalación del equipo en el bastidor.
- Energización del equipo.
- Verificación de las pruebas de Inicio (boot).
- Configuración de los parámetros básicos IP de las interfaces.
- Pruebas de conectividad.
- Configuración de Redes Virtuales en Conmutadores de acceso.
- Configuración de PortFast.
- Configuración de VTP.
- Configuración de SNMP.
- Configuración de Ether canales
- Configuración de seguridad para el acceso remoto.

4.6.1.2 Actualización de Imagen LAN Base a Ip Base en Conmutador Cisco 4507R.

- Verificación de parámetros antes de actualización de Imagen.
- Respaldo de Configuraciones.

- Actualización de IOS.
- Encendido del equipo y verificación del POST.
- Configuración de Redes Virtuales y Enrutamiento entre Redes Virtuales.
- Instalación de tarjeta WS-X4424-GB-RJ45
- Instalación de tarjeta WS-X4506-GB-T
- Configuración de PortFast.
- Configuración de VTP.
- Configuración de SNMP.
- Configuración de Ether canales
- Configuración de seguridad para el acceso remoto.
- Pruebas de conectividad

4.6.2 Plan de Implementación de la Red WAN

4.6.2.1 Instalación y configuración de Enrutador en la WAN (Hospital).

- Reunión para definir parámetros de instalación.
- Instalación de Enrutador Cisco 2911 en el bastidor
- Encendido de Enrutador Cisco 2911.
- Configuración de las Interfaces definidas en la reunión.
- Configuración de OSPF.

- Configuración de nuevas rutas estáticas (Conectividad de los usuarios de las nuevas redes virtuales con los servidores centrales)
- Pruebas de conectividad
- Documentación de la implementación.

4.6.2.2 Configuración de Enrutadores en la WAN.

- Respaldo de Configuraciones.
- Configuración de OSPF (Conectividad de los usuarios de las nuevas redes virtuales con los servidores centrales).
- Pruebas de conectividad.
- Documentación de la implementación.

4.6.3 Plan de Implementación de Software de Gestión y Monitoreo

4.6.3.1 Instalación de LMS 4.0 e Ingreso de Dispositivos.

- Reunión para definir parámetros de configuración.
- Instalación de Servidor en el rack DL-180.
- Instalación de Sistema Operativo.
- Instalación de LMS 4.0
- Documentación de la implementación.

4.7 Implementación de la Red LAN

4.7.1 Conmutador de Núcleo/Agregación Cisco 4500

Para la implementación de la red LAN se debe realizar configuraciones en el equipo Cisco 4507 a nivel de actualización de la imagen de las tarjetas supervisoras.

Este documento detalla el procedimiento a seguir para realizar la actualización de IOS en el dispositivo Cisco 4507R.

4.7.1.1 Pre requisitos

Se recomienda tener conocimientos sobre los siguientes tópicos:

- TFTP y como transferir archivos con este protocolo. Entendimiento de cómo configurar una PC para ser TFTP server.
- La imagen de software de IOS en la PC que será server TFTP.
- Verificación de conectividad y servicios disponibles, se deberá guardar el resultado de los siguientes comandos para verificaciones posteriores al cambio de IOS.

show run
show vlan
sh ip inter brief
sh ip route
sh proce cpu
sh module
sh tech sup

4.7.1.2 Procedimiento de Actualización de IOS

- Levantamiento de Servidor TFTP
- Nueva versión de IOS
- Verificación de espacio disponible en memoria flash
- Carga de nueva versión de IOS cat4500-ipbasek9-mz.122-54.SG.bin
- Verificación de variable boot
- Cambio de variable boot
- Cambios en configuración de redundancia
- Ejecución de recarga de tarjeta procesadora pasiva
- Ejecución de contingencia.
- Verificación de instalación de nueva imagen.
- Verificación de servicios y archivo de configuración.

4.7.1.3 Detalle de la Implementación

- Levantamiento de Servidor TFTP.

  Se debe conectar una PC con el direccionamiento correcto de forma de tener plena visibilidad del equipo. Probar la conectividad con el equipo realizando un Ping a la IP del equipo.

- Disponibilidad de la nueva versión de IOS.

  Tener el IOS a cargarse cat4500-ipbasek9-mz.122-54.SG.bin, en un directorio disponible para ser enviado vía TFTP.

- Verificación de espacio disponible en memoria flash en ambas supervisoras.

- Carga de nueva versión de IOS cat4500-ipbasek9-mz.122-54.SG.bin en ambas supervisoras.

Se debe utilizar el siguiente comando para copiar la imagen de IOS a la supervisora activa:

Switch#copy tftp bootflash:

Se debe utilizar el siguiente comando para copiar la imagen de IOS a la supervisora pasiva:

Switch#copy tftp slavebootflash:

En este punto las dos supervisoras tienen cargada la nueva imagen de IOS, aunque todavía se encuentra activa la imagen anterior. Se debe verificar que estén copiadas las nuevas imágenes que se cargaron, utilizar el comando:

Switch#dir all

Verificación de la variable de boot

Se debe verificar con que imagen esta arrancando el sistema, utilizar los siguientes comandos:

Switch#show bootvar

BOOT variable = bootflash: cat4000-i9k91s-mz.122-25.EWA12.bin,1

CONFIG_FILE variable =
BOOTLDR variable = bootflash: cat4500-boot-mz.122-25.SG
Configuration register is 0x102.

Switch#show run
Building configuration...

Current configuration : 1625 bytes
!
version 12.1
service timestamps debug datetime msec localtime
!
hostname c-MSFC15
!
boot system bootflash:cat4500-entservices-mz.122-53.SG

Cambio de la variable de boot y configuración de registro. Para la eliminación de la variable de boot antigua utilizar el siguiente comando:

Switch(config)#no boot system bootflash: cat4000-i9k91s-mz.122-25.EWA12.bin

Para definir la nueva variable de boot utilizar el siguiente comando:

Switch(config)# boot system bootflash: cat4500-ipbasek9-mz.122-54.SG.bin

Cambio en la configuración de registro:

Switch(config)#config-register 0x2

Cambio en la configuración de la redundancia, Para este paso se debe cambiar la configuración de la redundancia, se deben ingresar los siguientes comandos:

Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-syn standard
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The bootvar has been successfully synchronized to the
standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The config-reg has been successfully synchronized to
the standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The startup-config has been successfully synchronized

to the standby supervisor
4d01h: %C4K_REDUNDANCY-5-CONFIGSYNC: The private-config has been successfully synchronized
to the standby supervisor
Switch# copy running-config start-config

Ejecución de una recarga de la tarjeta secundaria. En este caso, se reinicializa la tarjeta secundaria, con el fin de que arranque con la nueva configuración.

Switch# redundancy reload peer

Ejecución de un conmutación para que la tarjeta supervisora secundaria entre al estado activo, y la antigua tarjeta primaria reinicie con nueva configuración.

Switch# redundancy force-switchover

Verificación de que los equipos arrancaron con la nueva imagen

Switch#show bootvar
BOOT variable = bootflash: cat4500-ipbasek9-mz.122-54.SG.bin,,1
CONFIG_FILE variable =
BOOTLDR variable = bootflash: cat4500-boot-mz.122-53.SG
Configuration register is 0x2101

Se recomienda validar el levantamiento de los servicios y utilizar los comandos sugeridos en los prerrequisitos para generar nueva información a ser comparada con el resultado de los comandos inicialmente requeridos.

4.7.1.4 Procedimiento de Recuperación en Caso de Actualización Fallida

En el caso de que no se haya borrado la imagen antigua, es decir se mantengan tanto la imagen antigua como la nueva en la memoria flash, se debe ejecutar el siguiente procedimiento.

Si por razones de espacio, se ha borrado la imagen antigua, se deberá borrar la imagen de IOS actualmente instalada, utilizando los siguientes comandos.

Switch#delete bootflash: cat4500-ipbasek9-mz.122-54.SG.bin
Switch#delete slavebootflash: cat4500-ipbasek9-mz.122-54.SG.bin

Posteriormente se debe copiar a las supervisoras la imagen originalmente instalada:

Switch#copy tftp bootflash:

Se debe utilizar el siguiente comando para copiar la imagen de IOS a la supervisora standby.

Switch#copy tftp slavebootflash:

4.7.1.5 Configuración Final de Conmutador de Núcleo/Agregación.

A continuación se entrega la configuración del Conmutador de Núcleo implementada la alta disponibilidad de las supervisoras y la doble conexión por cada Conmutador de acceso.

```
Sw1PBCore#
Sw1PBCore#wr
Building configuration...
Compressed configuration from 4389 bytes to 1726 bytes[OK]
Uncompressed configuration from 1726 bytes to 4389 bytes
Sw1PBCore#terminal len 0
Sw1PBCore#show run
Building configuration...

Current configuration : 4389 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service compress-config
!
hostname Sw1PBCore
!
boot-start-marker
boot-end-marker
!
redundancy
mode sso
enable secret 5 $1$Roub$4wNqkkQMHlgsJtc1Hjt6P1
!
username ibm privilege 15 password 7 020F06561F030231
no aaa new-model
clock timezone GMT -5
ip subnet-zero
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
vtp domain HOSPI_SUC1
vtp mode server
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet2/1
!
interface GigabitEthernet2/2
!
interface GigabitEthernet3/1
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet3/2
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/3
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/4
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/5
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/6
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/7
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/8
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/9
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/12
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/13
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/14
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/15
```

```
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/19
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/21
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/22
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/23
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/24
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet4/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet4/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet4/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
```

```
!
interface GigabitEthernet4/4
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 4 mode active
!
interface GigabitEthernet4/5
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 5 mode active
!
interface GigabitEthernet4/6
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 6 mode active
!
interface GigabitEthernet5/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet5/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet5/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet5/4
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 4 mode active
!
interface GigabitEthernet5/5
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 5 mode active
!
interface GigabitEthernet5/6
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 6 mode active
!
interface GigabitEthernet6/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 7 mode active
!
interface GigabitEthernet6/2
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
channel-group 7 mode active
!
interface GigabitEthernet6/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 8 mode active
!
interface GigabitEthernet6/4
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 8 mode active
!
interface GigabitEthernet6/5
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
!
interface GigabitEthernet6/6
switchport mode access
media-type rj45
!
interface GigabitEthernet7/1
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/2
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/3
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/4
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/5
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/6
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/7
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/8
 switchport mode access
 spanning-tree portfast
```

```
!
interface GigabitEthernet7/9
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/12
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/13
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/14
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/15
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/16
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/19
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/21
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet7/22
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/23
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet7/24
 switchport mode access
 spanning-tree portfast
!
interface Port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 4
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 5
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 6
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 7
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel 8
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 172.18.1.1 255.255.255.0
!
no ip http server
line con 0
```

```
exec-timeout 120 0
logging synchronous
login local
stopbits 1
line vty 0 4
exec-timeout 0 0
password 7 121A0C041104
login local
length 0
transport input telnet
```

4.7.2 Configuración final de Conmutadores de Acceso

Se presenta la salida del comando Show running-config:

```
Switch#SHOW RUNN
Building configuration...

Current configuration : 1244 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
vtp client
vtp domain HOSPI_SUC1
!
interface FastEthernet0/1
spanning-tree portfast
switchport access vlan 10
!
interface FastEthernet0/2
spanning-tree portfast
switchport access vlan 10
!
interface FastEthernet0/3
spanning-tree portfast
switchport access vlan 10
!
interface FastEthernet0/4
spanning-tree portfast
switchport access vlan 10
!
interface FastEthernet0/5
spanning-tree portfast
switchport access vlan 10
!
```

```
interface FastEthernet0/6
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/7
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/8
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/9
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/10
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/11
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/12
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/13
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/14
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/15
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/16
spanning-tree portfast
switchport access vlan 40
!
interface FastEthernet0/17
spanning-tree portfast
switchport access vlan 40
!
interface FastEthernet0/18
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/19
```

```
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/20
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/21
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/22
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/23
spanning-tree portfast
switchport access vlan 20
!
interface FastEthernet0/24
spanning-tree portfast
switchport access vlan 20
!
interface GigabitEthernet1/1
channel-group 1 mode active
switchport mode trunk
!
interface GigabitEthernet1/2
channel-group 1 mode active
switchport mode trunk
!
interface Port-channel 1
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
172.18.1.13 255.255.255.0
!
ip default-gateway 172.18.1.250
!
```

4.8 Implementación de la Red WAN

A continuación se detalla la configuración de la solución WAN con un esquema de redundancia en la WAN implementando OSPF.

4.8.1 Configuración final de Enrutador de la WAN Hospital

Se presenta la salida del comando Show Running-config:

```
#sh run
Building configuration...
Current configuration : 2229 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname XXXXXXXXXX
!
logging rate-limit console 10 except errors
enable secret 5 $1$GCWF$6e2kCWZNjlJv9z3yYMdli/
enable password 7 060506324F41
!
username Cisco privilege 15 password 7
00404242330A0D274B2E1D413A3C15161A221B221C0D153B31022C
username administrador privilege 15 password 7 094D4A044A5542000C
clock timezone GMT -5
ip subnet-zero
no ip domain-lookup
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
interface Loopback0
 ip address 10.10.10.11 255.255.255.255
!
interface GigaEthernet0/0
ip address 192.168.254.2 255.255.255.252
duplex auto
speed auto
!
interface GigaEthernet0/1
 ip address 192.168.254.30 255.255.255.252
 duplex auto
 speed auto
!
interface GigaEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface GigaEthernet0/2.1
 encapsulation dot1Q 13
```

```
 ip address 172.18.4.1 255.255.255.0
!
interface GigaEthernet0/2.2
 encapsulation dot1Q 11
 ip address 172.18.2.1 255.255.255.0
!
interface GigaEthernet0/2.3
 encapsulation dot1Q 10
 ip address 172.18.1.1 255.255.255.0
!
interface GigaEthernet0/2.4
 encapsulation dot1Q 20
 ip address 172.18.11.1 255.255.255.0
!
interface GigaEthernet0/2.5
 encapsulation dot1Q 21
 ip address 172.18.12.1 255.255.255.0
!
router ospf 10
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.254.0 0.0.0.255 area 0
!
ip classless
!
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
no cdp run
!
snmp-server community public RO
snmp-server location Hospital XXXXX
!
banner login ^C
**************************************************
*    HOSPITAL                                    *
*                                                *
*           - XXXXXXXXXX -                       *
*  ACCESOS NO AUTORIZADOS ESTAN PROHIBIDOS       *
*          Y SERAN REPORTADOS!!!                 *
**************************************************
^C
!
line con 0
exec-timeout 120 0
logging synchronous
login local
stopbits 1
line vty 0 4
exec-timeout 0 0
password 7 121A0C041104
```

```
login local
length 0
transport input telnet
!
scheduler max-task-time 5000
end
```

4.8.2 Configuración Base de Enrutadores.

Se presenta la salida del comando Show Running-config:

```
#sh run
Building configuration...
Current configuration : 2229 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname XXXXXXXXXX
!
logging rate-limit console 10 except errors
enable secret 5 $1$GCWF$6e2kCWZNjlJv9z3yYMdli/
enable password 7 060506324F41
!
username Cisco privilege 15 password 7
00404242330A0D274B2E1D413A3C15161A221B221C0D153B31022C
username administrador privilege 15 password 7 094D4A044A5542000C
clock timezone GMT -5
ip subnet-zero
no ip domain-lookup
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
interface Loopback0
 ip address 10.10.10.12 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.254.1 255.255.255.252
duplex auto
speed auto
!
interface Ethernet0/1
 ip address 192.168.254.5 255.255.255.252
 duplex auto
```

```
 speed auto
!
interface Ethernet0/2
 no ip address
 duplex auto
 speed auto
!
interface Ethernet0/2.1
 encapsulation dot1Q 10
 ip address 172.18.1.250 255.255.255.0
!
interface Ethernet0/2.2
 encapsulation dot1Q 11
 ip address 172.18.2.250 255.255.255.0
!
!
interface Ethernet0/2.3
 encapsulation dot1Q 12
 ip address 172.18.3.250 255.255.255.0
!
interface Ethernet0/2.4
 encapsulation dot1Q 13
 ip address 172.18.4.250 255.255.255.0
!
interface Ethernet0/2.5
 encapsulation dot1Q 14
 ip address 172.18.5.250 255.255.255.0
!
interface Ethernet0/2.6
 encapsulation dot1Q 15
 ip address 172.18.6.250 255.255.255.0
!
interface Ethernet0/2.7
 encapsulation dot1Q 16
 ip address 172.18.7.250 255.255.255.0
!
interface Ethernet0/2.8
 encapsulation dot1Q 17
 ip address 172.18.8.250 255.255.255.0
!
interface Ethernet0/2.9
 encapsulation dot1Q 18
 ip address 172.18.9.250 255.255.255.0
!
interface Ethernet0/2.10
 encapsulation dot1Q 19
 ip address 172.18.10.250 255.255.255.0
!
interface Ethernet0/2.8
 encapsulation dot1Q 20
 ip address 172.18.11.250 255.255.255.0
!
router ospf 10
```

```
 log-adjacency-changes
 network 172.18.0.0 0.0.255.255 area 0
 network 192.168.254.0 0.0.0.255 area 0
!
ip classless
!
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
no cdp run
!
snmp-server community public RO
snmp-server location Hospital Gilbert
!
banner login ^C
**************************************************
*   REFERENCIA                                   *
*                                                *
*          - XXXXXXXXXX -                        *
*  ACCESOS NO AUTORIZADOS ESTAN PROHIBIDOS       *
*         Y SERAN REPORTADOS!!!                  *
**************************************************
^C
!

line con 0
exec-timeout 120 0
logging synchronous
login local
stopbits 1
line vty 0 4
exec-timeout 0 0
password 7 121A0C041104
login local
length 0
transport input telnet
!
scheduler max-task-time 5000
```

4.9 Implementación del Sistema de Monitoreo y Gestión.

Los prerrequisitos para instalar Cisco LMS 4.0 en Windows son los siguientes:

- El servidor cumple con los requerimientos de hardware y software, ver cuadro N° 18.

- Se debe desactivar el Servicios de Terminal Server en el sistema operativo Windows en el modo de aplicación.
- Si se ha habilitado Terminal Server en modo de aplicación, desactive el servidor de Terminal Server, reinicie el sistema, y comenzar de nuevo la instalación. Sin embargo, puede habilitar Servicios de Terminal Server en modo de administración remota.
- Si ha configurado colector Syslog remoto (RSC) en un servidor diferente, debe actualizar de RSC a RSC 5.1. Consulte la Instalación del colector de Syslog remoto para más información.
- Ha desactivado el antivirus en su sistema durante la instalación.
- Se ha configurado el espacio de intercambio recomendado. Ver Requisitos del sistema del navegador del servidor y el cliente para más información.

Cuadro N° 26

Requerimientos de Hardware y Software para instalación de LMS 4.0

COMPONENTE	REQUERIMIENTO RECOMENDADOS DEL SISTEMA SERVIDOR
LMS 100	1 CPU CON DUAL CORE O 2 CPU CON 4GB DE RAM Y 8 GB DE SWAP , 60 GB DE ESPACIO EN DISCO CON SISTEMA OPERATIVO DE 32 O 64 BITS
SISTEMA OPERATIVO	WINDOWS 2008 STANDARDT O ENTERPRISE EDITION RELEASE 1 CON SP1 Y SP2 PARA 32 BITS
	WINDOWS 2008 STANDARDT O ENTERPRISE EDITION RELEASE 2 CON SP1 PARA 64 BITS

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

Se instaló y configuró la herramienta de monitoreo Cisco LMS 4.0 con licencia permanente para 100 dispositivos. En la misma se ingresaron 3 dispositivos para mostrar su funcionalidad y el registro de los demás dispositivos corre por cuenta del cliente. Para ello se realizó un manual de usuario denominado "Ingreso de nuevos dispositivos al Cisco Works.html"

Gráfico N°27 : Instalación de Software de Monitoreo LMS
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Se creó y configuró los siguientes usuarios para la correcta instalación de la aplicación.

Cuadro N° 27

Usuarios para Instalación de LMS 4.0

Usuario	Password
Admin	Tdsprht2012
Guest	Viewnet
Casuser	Toolnet2011
Data Base	DBAcworks

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

La siguiente figura muestra la topología que forman los dispositivos una vez ingresados y reconocidos por la herramienta.

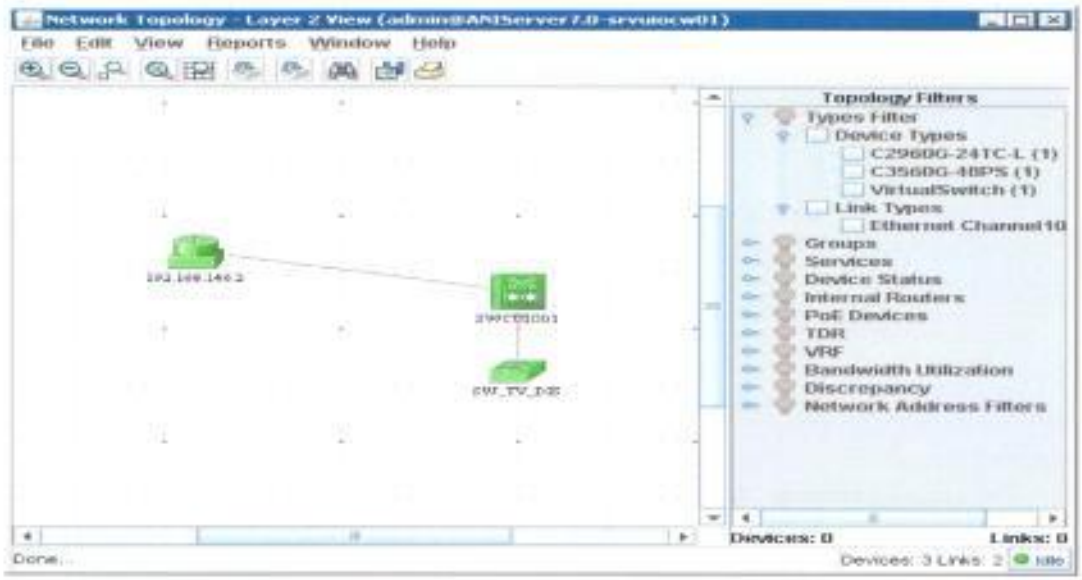


Gráfico N°28 : Diagrama de red utilizando software de Monitoreo LMS
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Para ello deben ser creadas comunidades de snmp en todos los dispositivos CISCO que requieran ser monitoreados, apuntar a la dirección del Cisco LMS instalado y habilitar las alertas de snmp que van a ser enviados.

```
snmp-server community rtvecrw RW
snmp-server community rtvecro RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps mac-notification
```

```
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 172.16.8.100 rtvecr
```

4.10 Fotos de la Implementación

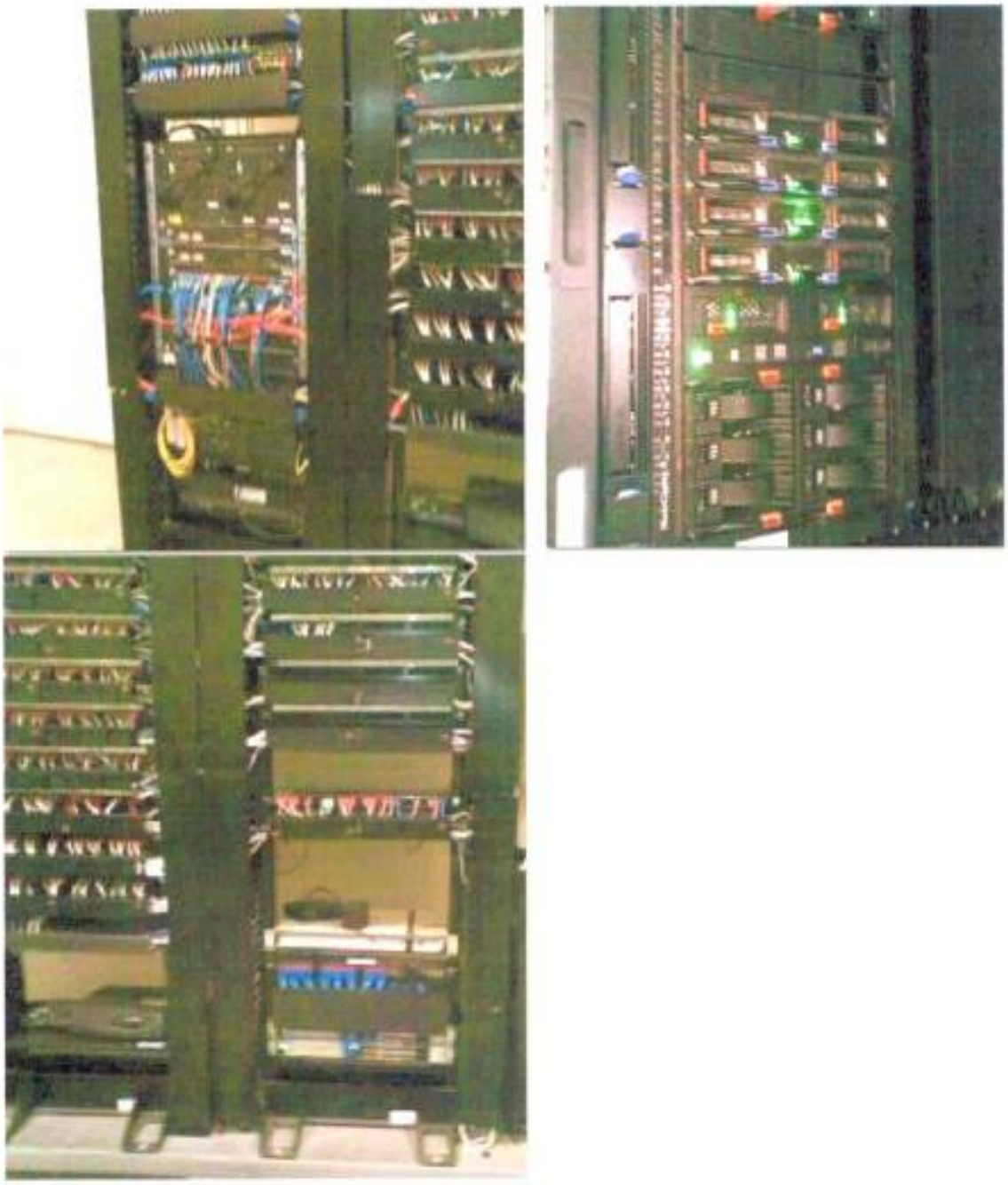


Gráfico N°29 : Cisco 4507R, Servidores y Conmutadores de Acceso
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

CAPITULO 5

PRUEBAS DE ALTA DISPONIBILIDAD DE LA NUEVA RED

5.1 Pruebas de Alta Disponibilidad WAN

A continuación se detalla los objetivos de las pruebas realizadas en la WAN.

5.1.1 Objetivos:

- Validar las configuraciones aplicadas a los equipos instalados en las localidades de Oficina central y Hospital 1 donde se cambia los conmutadores y se les aplica la alta disponibilidad.
- Validar la implementación OSPF en la WAN, por lo cual se simulara la caída de enlaces y la operatividad de la red ante estos eventos de cambios de topologías.

5.1.2 Procedimiento

A continuación se describe el procedimiento mediante el cual se validarán los objetivos de antes descritos.

- Interfaces de conectividad estén en modo operativo.

Para esto luego de haber configurado los enrutadores se digitará el comando show ip interface brief, con el cual se verificará el estado activo y el protocolo activo en las interfaces WAN que comunican hacia las demás localidades.

- Que se tenga conectividad desde un pc de la oficina central hacia un pc ubicado en las distintas oficinas.

  Para ello se abrirá una pantalla de DOS en una PC ubicada en Oficina central y se dará ping a PC ubicada en las otras localidades.

  Luego se procede a simular falla en los enlaces ingresando en los enrutadores y en las interfaces de conectividad con los enlaces de radio se dará el comando (**router(config-if)# shutdown**).

  Se deberá observa una pequeña perdida de conectividad debido a la convergencia del protocolo de enrutamiento, pero el mismo no debe ser mas allá de 2 segundos y luego seguir operando normalmente.

  En las pc se abrirá una pantalla de DOS y se ejecutara el comando ping en formato extendido (**C:\Users\>ping <dir ip> -t**) para verificar dicha conectividad.

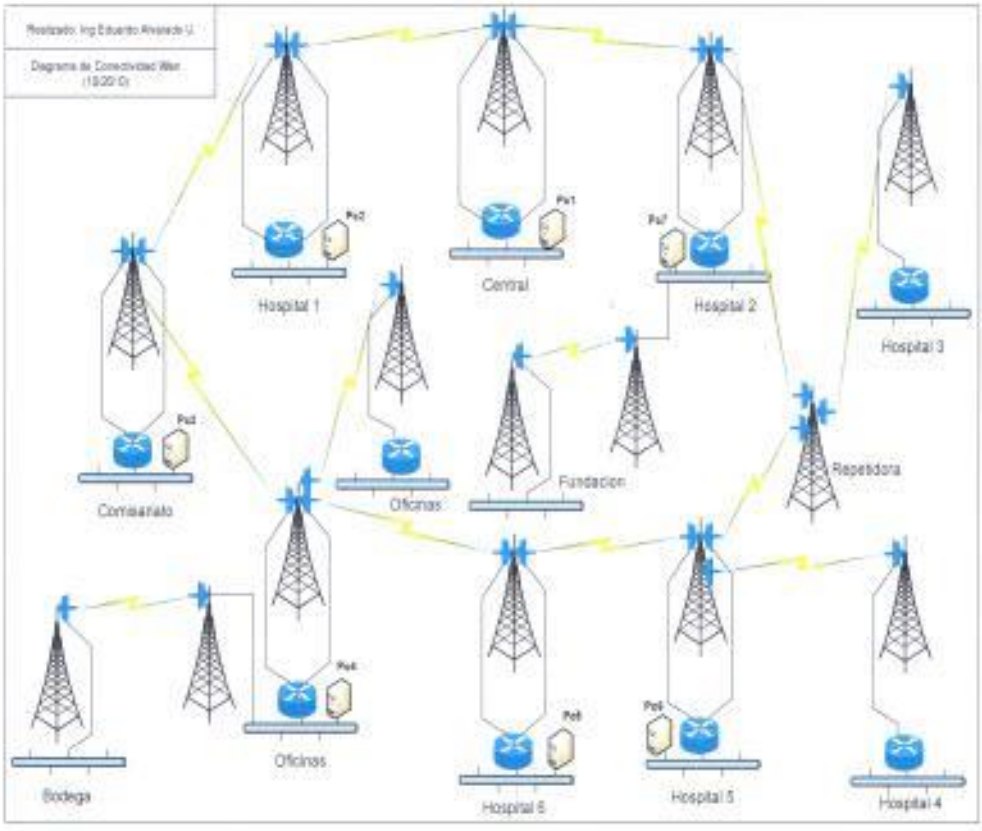


Gráfico N°30 : Diagrama de la red utilizada para las pruebas WAN
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Se adjunta la tabulación de las pruebas

Cuadro N° 28

Resultado de plan de pruebas de la red WAN

PLAN DE PRUEBAS DE LA RED WAN		
Verificación de conectividad con el anillo de enlaces de radio	**Pasa**	**Falla**
Ping Verificación de conectividad de oficina central con hospital 1 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 2 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 5 (paquetes de 64 bytes)	x	

Ping Verificación de conectividad de oficina central con hospital 6 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con Comisariato (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con oficinas (paquetes de 64 bytes)	x	
Verificación de conectividad con el anillo de enlaces de radio ante perdida de enlace central - hospital 1	**Pasa**	**Falla**
Ping Verificación de conectividad de oficina central con hospital 1 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 2 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 5 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 6 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con Comisariato (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con oficinas (paquetes de 64 bytes)	x	
Verificación de conectividad con el anillo de enlaces de radio ante perdida de enlace hospital 5 - hospital 6	**Pasa**	**Falla**
Ping Verificación de conectividad de oficina central con hospital 1 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 2 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 5 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con hospital 6 (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con Comisariato (paquetes de 64 bytes)	x	
Ping Verificación de conectividad de oficina central con oficinas (paquetes de 64 bytes)	x	

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

5.2 Pruebas de Alta Disponibilidad LAN

A continuación se detallan los objetivos de las pruebas de conectividad LAN.

5.2.1 Objetivo

Validar que las configuraciones aplicadas a los equipos funcionen correctamente, para lo cual se validará:

- Verificar la alta disponibilidad en las supervisoras del conmutador de Núcleo/Agregación Cisco 4507R.
- Verificar la alta disponibilidad en las fuentes de poder.
- Verificar la redundancia en las tarjetas hacia los conmutadores de acceso.
- Verificar la redundancia en las tarjetas hacia los servidores.
- La red virtual de administración esté en modo operativo.
- La conectividad hacia el enrutador por defecto de la red LAN.
- Que el conmutador esté configurado correctamente los parámetros de VTP tales como: nombre del dominio, modo de trabajo y contraseña.
- Que el servidor VTP propague las redes virtuales del dominio.
- Se tenga conectividad hacia el Conmutador de Núcleo/Agregación.
- Que los usuarios accedan a los servicios de la red

5.2.2 Procedimiento

A continuación se describe el procedimiento mediante el cual se validarán los objetivos de antes descritos.

- Alta disponibilidad de Supervisoras

  Para esto verificar el funcionamiento con el comando **show redundancy states** y el comando **redundancy force-switchover** para forzar manualmente el switchover a la otra supervisora.

  Primero deberá forzar manualmente a que se sincronicen los archivos de configuración de las dos supervisoras.

  Switch(config)# redundancy
  Switch(config-red)# main-cpu
  Switch(config-r-mc)# auto-sync standard
  Switch(config-r-mc)# end
  Switch# copy running-config startup-config.

- Alta disponibilidad en las fuentes de poder

  Para verificar la alta disponibilidad de las fuentes de poder utilizar el comando **show power, show power supplies.**

- Alta disponibilidad de los puertos de conexión hacia los conmutadores de acceso y servidores.

  Si se desea habilitar toda la tarjeta ejecutar el siguiente comando **Switch(config)# no hw-module module x power,** para validar la correcta operación de los ether canales se pueden utilizar los siguientes comandos

show etherchannel x port-channel, show cdp neighbors, show interfaces fastethernet x etherchannel.

- Que la red virtual de administración esté en modo operativo.

  Para esto luego de haber configurado el Conmutador se digitará el comando **show ip interface brief**, con el cual se verificará el **estado activo** y el **protocolo activo** en la vlan de administración. En todas las localidades se debe verificar el estado de las **Vlans x, y, z**.con el comando **show vlan**

- Que se tenga conectividad hacia el enrutador para la red LAN.

  Observando las configuraciones de cada uno de los PC de acceso se debe hacer ping a su **default-gateway**.

- Que el Conmutador esté configurado correctamente los parámetros de VTP tales como: nombre del dominio, modo de trabajo y contraseña.

  Para esto nos ayudaremos de los comandos **show vtp status** y **show vtp password**. Estos comandos se deberán ejecutar para validar que la misma configuración tenga tanto el Conmutador en producción como su remplazo.

- Que el servidor VTP propague las redes virtuales del dominio.

  Para validar que las redes virtuales se hayan propagado en el Conmutador que se remplaza se digitará el comando **show vlan**, y se verificarán las vlan's propagadas con las que el Conmutador que estaba en producción tenga.

- Que se tenga conectividad remota al equipo por fines administrativos.

Estableciendo una sesión de telnet hacia la misma dirección del equipo e ingresando el usuario y contraseña local de administración.

- Que los usuarios accedan a los servicios de la red.

  Para verificar este servicio se deberá probar en una PC disponible con los aplicativos de los usuarios del sistema.

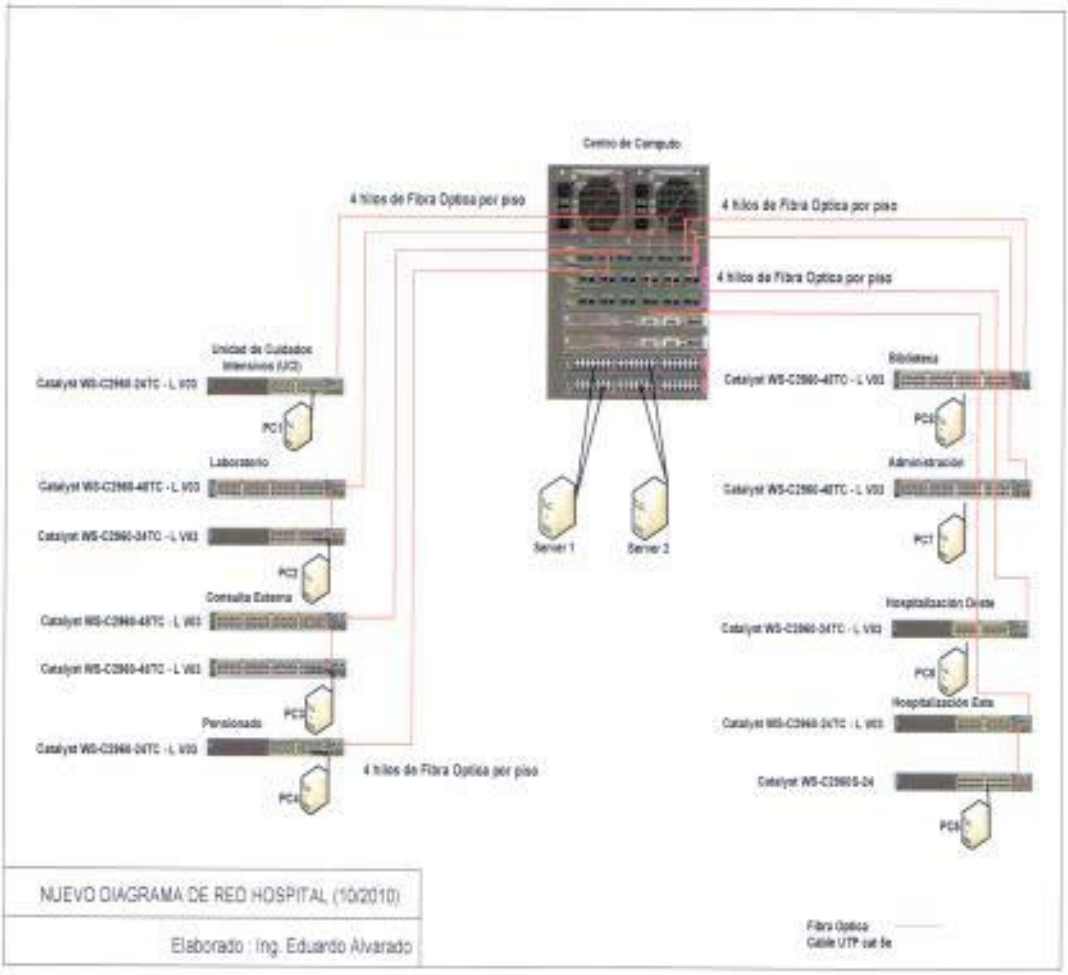


Gráfico N°29 : Diagrama de la red utilizada para las pruebas LAN
Fuente : Datos de la investigación
Elaboración : Eduardo Alvarado

Se adjunta la tabulación de las pruebas.

Cuadro N° 29

Resultado de Plan de Pruebas de la Red LAN

Pruebas de alta disponibilidad de la Procesadora	**Pasa**	**Falla**
Accede por CLI al equipo 4507R	x	
Deshabilitar Supervisora 1	x	
Automáticamente se activa Supervisora 2	x	
Se pierde conectividad entre Pc1 y PC2	x	
Verificación de acceso a 4507R	x	
Activación de Supervisora 1	x	
Deshabilitar Supervisora 2	x	
Se pierde conectividad entre Pc1 y PC2	x	
Activación de Supervisora 2	x	
Verificación de operatividad completa del equipo	x	
Pruebas de alta disponibilidad de Fuente de Poder	**Pasa**	**Falla**
Accede por CLI al equipo 4507R	x	
Verificación que las fuentes de poder estén en configuración redundante	x	
Apagado manual de una fuente de poder 1 (Conmutador off)	x	
Se pierde conectividad entre Pc1 y PC2	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Encendido de la fuente 1 (Conmutador encendido)	x	
Verificación por CLI que las dos fuentes estén operativas y redundantes	x	
Apagado manual de la segunda fuente de poder 2 (Conmutador apagado)	x	
Hay conectividad entre Pc1 y PC2	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Pruebas de alta disponibilidad de Tarjeta de Conmutadores de Acceso	**Pasa**	**Falla**
Accede por CLI al equipo 4507R	x	
Verificación de operatividad de todos los puertos de Conmutadores de Acceso	x	
Apagado manual de todos los puertos de acceso de la tarjeta del Slot (shutdown)	x	

Hay conectividad entre PC1 - PC2, PC1 - PC3, PC1 - PC4, PC1 - PC5, PC1 - PC6, PC1 - PC7, PC1 – PC8	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Encendido de todos los puertos de acceso de la tarjeta del Slot (no Shutdown)	x	
Hay conectividad entre PC1 - PC2, PC1 - PC3, PC1 - PC4, PC1 - PC5, PC1 - PC6, PC1 - PC7, PC1 – PC8	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Apagado manual de todos los puertos de acceso de la tarjeta del Slot (shutdown)	x	
Hay conectividad entre PC1 - PC2, PC1 - PC3, PC1 - PC4, PC1 - PC5, PC1 - PC6, PC1 - PC7, PC1 – PC8	x	
Encendido de todos los puertos de acceso de la tarjeta del Slot (no Shutdown)	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Pruebas de alta disponibilidad de Tarjeta de Servidores	**Pasa**	**Falla**
Accede por CLI al equipo 4507R	x	
Verificación de operatividad de todos los puertos de Conmutadores de Acceso	x	
Apagado manual de todos los puertos de acceso de ala tarjeta del Slot (shutdown)	x	
Hay conectividad entre PC1 - Server 1, PC1 - Server 2, PC1 - Server 3	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Encendido de todos los puertos de acceso de la tarjeta del Slot (no Shutdown)	x	
Hay conectividad entre PC1 - Server 1, PC1 - Server 2	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Apagado manual de todos los puertos de acceso de ala tarjeta del Slot (shutdown)	x	
Hay conectividad entre PC1 - Server 1, PC1 - Server 2	x	
Encendido de todos los puertos de acceso de la tarjeta del Slot (no Shutdown)	x	
Verificación de acceso a 4507R y operatividad del equipo	x	
Pruebas de servicios configurados en conmutadores de acceso y núcleo/agregación	**Pasa**	**Falla**
Accede por CLI al equipo 4507R	x	
Verificación de operatividad de todos los puertos de los	x	

Conmutadores de acceso al conmutador de núcleo/agregación		
Verificación de las redes virtuales creadas en los conmutadores	x	
Creación de una red virtual de Prueba	x	
Verificación de creación automática de esta red virtual de prueba en el Conmutador de núcleo y acceso.	x	
Verificación del VTP server (Conmutador de Core).	x	
Verificación de los ether canales (grupos)	x	
Apagado manual de todos los puertos de acceso de ala tarjeta del Slot (shutdown)	x	
Hay conectividad entre PC1 - Server 1, PC1 - Server 2	x	
Verificación de los ether canales (grupos)	x	
Encendido de todos los puertos de acceso de la tarjeta del Slot (no Shutdown)	x	
Verificación de los PC de usuario a los sistemas del hospital	x	
Verificación de acceso al conmutador de núcleo/agregación 4507R y operatividad del equipo	x	

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

5.3 Pruebas de Monitoreo y Gestión de la Red

A continuación se detalla los resultados de las pruebas de monitoreo y gestión de dispositivos de la red LAN y WAN del hospital.

5.3.1 Objetivo

- Validar que las configuraciones aplicadas para que los equipos sean monitoreados y gestionados de acuerdo a los requerimientos del hospital, para lo cual se validará:

- Verificar que los dispositivos a ser gestionados envíen las alarmas SNMP a Cisco LMS.
- Verificar que los dispositivos cuando generen eventos los envíen a Cisco LMS.
- Verificar el descubrimiento de los dispositivos de red a través de Cisco LMS.
- Verificar la reportería de eventos de Cisco LMS.
- Verificar la actualización de configuraciones y respaldo de los mismos a través de Cisco LMS.
- Verificar la actualización de imagen a través de Cisco LMS.

5.3.2 Procedimiento

A continuación se describe el procedimiento mediante el cual se validarán los objetivos de antes descritos.

- Validación de traps recibidos en el Cisco LMS.

  En el servidor donde se encuentra instalado Cisco LMS navegar en Monitor > Monitoring Tools > Fault Monitor.

- Validación de dispositivos generados por dispositivos.

En el Conmutador de core se generara un evento (desconectando un PC activo de un puerto del Conmutador) y se verificara en el fault monitor si se reciben los eventos generados.

En el servidor donde se encuentra instalado Cisco LMS navegar en Monitor > Monitoring Tools > Fault Monitor > Device Fault Sumary

- Validación de descubrimiento de dispositivos.

  Se deberá validar el ingreso de un dispositivo en el siguiente path Resource Manager Essentials > Devices > Device Management > RME Devices

- Validación de reporteria en Cisco LMS.

  Para la validación de la reporteria ingresar en el siguiente path Reports > Report Archives > Inventory and Syslog

- Validación de actualizaciones de configuraciones y respaldos.

  Para la validación de las actualizaciones de software y Admin > Network > Software Image Management > View/Edit Preferences.

  En el dispositivo se deberá ingresar el comando **show versión** para verificación de las imágenes cargadas

Cuadro N° 30

Resultado de plan de pruebas de monitoreo y gestión

Pruebas de generación de alarmas y recepción de los mismos en Cisco Lms	**Pasa**	**Falla**
Acceder a Cisco LMS	x	
Verificación en Cisco LMS la bitácora de traps recibidos	x	
Generación de eventos un puerto de prueba de Conmutador de Core (conexión y desconexión del puerto)	x	
Verificación de la recepción de estos eventos en el Cisco Lms	x	
Lectura de los eventos generados en el Cisco Lms	x	
Pruebas de descubrimientos de dispositivos y validación de reporteria	**Pasa**	**Falla**
Acceder a Cisco Lms.	x	
Ingreso de un dispositivo de prueba a través de una IP valida y la correcta configuración de SNMP.	x	
Iniciar el descubrimiento del dispositivo a través de Ping (ICMP).	x	
Verificación del descubrimiento del dispositivo en Cisco Lms.	x	
Elaboración de reportes utilizando la herramienta de reporteria del Cisco Lms.	x	
Pruebas de distribución de Imágenes IOS en dispositivos a través de Cisco Lms.	**Pasa**	**Falla**
Acceder a Cisco Lms.	x	
Ingreso de una imagen valida de un Conmutador cisco 2960 en el repositorio de Cisco Lms	x	
Envió de actualización de IOS en Conmutador cisco 2960.	x	
Verificación de envió de imagen en Conmutador cisco Comando **show versión**	x	
Verificación de la funcionalidad del Conmutador	x	

Fuente : Datos de la investigación Hospital
Elaboración: Eduardo Alvarado

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

En la presente tesis se ha analizado que el sistema de red del hospital, no cuenta con esquemas de alta disponibilidad tanto en su red LAN como WAN. Si bien es cierto a nivel de comunicaciones en la WAN el hospital cuenta con la infraestructura necesaria la misma no funciona adecuadamente, por lo que muchos procedimientos para mantener la red funcionando son realizados manualmente.

En la red LAN se encontró lazos en la red de acceso, los mismos que fueron mitigados por el protocolo de Árbol Expandido. Pero dado que no se cuenta con un software de monitoreo y gestión de redes este tipo de eventos no pueden ser identificados proactivamente.

La carencia de un software de gestión de redes hace que la reacción ante eventos en la red solo sean reactivos y no proactivos en ocasiones enterándose de los problemas en la red cuando el usuario los llama a comunicarles de los problemas.

El objetivo principal de esta tesis fue el rediseño y la implementación de la red LAN y WAN para que el hospital goce de un sistema escalable y con alta disponibilidad

que permita implementar nuevos sistemas transaccionales para brindar servicios de calidad a sus pacientes.

En la parte LAN se potenció el Conmutador de Núcleo/Agregación, se implementó esquemas redundantes en las tarjetas de conexión hacia los conmutadores de acceso, de tal manera que ante falla de una de sus tarjetas la red siga funcionando de manera transparente para el usuario, así mismo el Conmutador de Núcleo/Agregación y sus componentes cuentan con contratos de garantía avanzada del fabricante 24x7x4 que permiten que se tenga una parte de remplazo en sitio en cuatro horas.

Para la conexión de los servidores se integró a este Conmutador una segunda tarjeta para permitir formar enlaces de doble conexión a los servidores con LACP.

En la red WAN se implementó una red redundante en anillo y se activó el protocolo de enrutamiento dinámico OSPF, se eligió la familia de los protocolos de enrutamiento de estado de enlace por su rápida convergencia. Con ello ante la falla de un enlace del anillo, el tráfico se interrumpe por pocos segundos y se vuelve a activar la comunicación entre todos los nodos.

Se implementó el sistema de gestión y monitoreo de Cisco LMS 4.0 dado que todos los equipos son de marca Cisco el mismo que permite realizar la gestión del respaldo de configuraciones y actualizaciones de IOS en los equipos de manera remota,

adicionalmente permitirá realizar acciones proactivas para medir la salud de los dispositivos de red.

Mediante la implementación de todo el hardware y software indicado se logro los parámetros de escalabilidad y alta disponibilidad deseados en la red del hospital.

6.2 Recomendaciones.

Tomando en consideración los resultados alcanzados en el proceso de rediseño e implementación de la red LAN y WAN del Hospital, se pueden resaltar una serie de recomendaciones.

La red diseñada del Hospital permite la implementación de IPv6, pues todos sus componentes activos de la red soportan este protocolo, que es hacia donde apuntan las nuevas aplicaciones.

La red esta diseñada para soportar aplicaciones de Multidifusión, tales como video y telemedicina para poder expandir los servicios del Hospital hacia otras localidades donde hacen falta especialistas médicos.

Esta diseñada para soportar calidad de servicio (QoS) para soportar el transporte de imágenes medicas en toda la red del Hospital.

A un futuro inmediato se recomienda implementar algún protocolo de alta disponibilidad de puerta de enlace tales como HSRP y GLBP, también es recomendable migrar el enlace de radio a un anillo de fibra óptica, para mejorar el ancho de banda entre la red hospitalaria.

En una fase posterior se requiere implementar seguridades a nivel de LAN como Network Access Control, para lograrlo los conmutadores soportan la funcionalidad de IEEE 802.1X. Esta solución permitirá controlar a los usuarios implementando perfiles de ingreso a la red.

A nivel WAN se podrá implementar la encriptación los datos que viajan en los enlaces de radio, utilizando módulos de encriptación en los enrutadores y cambiando las funcionalidades del IOS de los enrutadores.

Adicionalmente se puede implementar servicios de AAA como Radius y Tacas para realizar auditorias de los cambios de configuración realizados en los dispositivos de red.

Se recomienda promover un plan de migración de la infraestructura de los otros hospitales de la red adaptado a los lineamientos teóricos-prácticos desarrollados en esta investigación, para fortalecer las redes LAN y WAN en cada uno de ellos.

Finalmente se recomienda socializar los resultados de la investigación, con el propósito de valorarlos y crear conciencia de la importancia de contar con redes escalables y de alta disponibilidad para los hospitales en donde son tan críticos los servicios hospitalarios.

BIBLIOGRAFIA

Amir Ranjbar, Keith Hutton	Designing Cisco Network Architecture - Pearson Education, limited 2008, 696 páginas
Teresea C. Mann Piliouras	Network Design: Management and Technical Perspective - Edicion 2, 2004 Auerbach Publications , 674 paginas
Robert Padjen, Todd Lammle	CCDP: cisco Internetwork Design Study Guide, Sybex, 2008 , 580 páginas
Deepankar Medhi, Karthikeyan Ramasamy	Network Routing , Algorithms, Protocolols, and Architectures, Morgan Kaufmann
Mark A. Sportack	Ip Routing Fundamentals, cisco Press , 2010, 510 páginas
Steven Karris	Networks: Design and Managment , Orchard Publications, 2009, 522 páginas
Gabor Fichtinger, Anne Martel, Terry Peters	Medical Image Computing and Computer Assisted Intervention, Springer, 2011 , 699 páginas
Guy Davies	Designing and Developing Scalable Ip Networks, Jhon Wiley & Sons, 2009 , 302 páginas

NETGRAFIA

Cisco Systems http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html

Cisco Systems http://www.cisco.com/en/US/docs/solutions/Verticals/Healthcare/MGN_Campus.html

Cisco Systems http://www.cisco.com/en/US/docs/solutions/Verticals/Healthcare/MGN_2.0.html

Cisco Systems http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html

ANEXO 1

CONFIGURACION SWITCH DE CORE (INICIAL)

```
Sw1PBCore#
Sw1PBCore#wr
Building configuration...
Compressed configuration from 4389 bytes to 1726 bytes[OK]
Uncompressed configuration from 1726 bytes to 4389 bytes
Sw1PBCore#terminal len 0
Sw1PBCore#show run
Building configuration...
Current configuration : 4389 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service compress-config
!
hostname Sw1PBCore
!
boot-start-marker
boot-end-marker
!
!
redundancy
 mode sso
enable secret 5 $1$Roub$4wNqkkQMHIgsJtc1Hjt6P1
!
username ibm privilege 15 password 7 020F06561F030231
no aaa new-model
clock timezone GMT -5
ip subnet-zero
!
!
!
!
no file verify auto
spanning-tree mode pvst
```

```
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet2/1
!
interface GigabitEthernet2/2
!
interface GigabitEthernet3/1
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/2
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/3
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/4
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/5
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/6
 switchport mode access
 spanning-tree portfast
!
```

```
interface GigabitEthernet3/7
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/8
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/9
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/11
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/12
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/13
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/14
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/15
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/16
 switchport mode access
 spanning-tree portfast
```

```
!
interface GigabitEthernet3/17
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/18
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/19
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/21
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/22
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/23
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet3/24
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet4/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet4/2
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
!
interface GigabitEthernet4/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet4/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet4/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet4/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet5/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet5/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet5/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
!
interface GigabitEthernet5/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
!
interface GigabitEthernet5/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 media-type rj45
!
interface GigabitEthernet5/6
 switchport mode access
 media-type rj45
!
interface Vlan1
 ip address xxx.xxx.xxx.xxx 255.255.255.0
!
ip default-gateway xxx.xxx.xxx.xxx
no ip http server
!
!
!
!
banner login ^C
**************************
9w2d: %C4K_REDUNDANCY-5-CONFIGSYNC: The startup-config has been successfully
synchronized to the standby supervisor
9w2d: %C4K_REDUNDANCY-5-CONFIGSYNC: The private-config has been successfully
synchronized to the standby supervisor**********************
*                               *
*   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx    *
*      xxxxxxxxxxxxxxxxxxxxxxx       *
*                               *
*            SW1PBCore          *
*        - ACCESO RESTRINGIDO -       *
*                               *
***********************************************
^C
!
line con 0
 logging synchronous
 login local
 stopbits 1
line vty 0 4
 logging synchronous
 login local
!
```

```
!
end

Sw1PBCore#show clock
*10:01:20.124 GMT Thu Dec 9 2010
Sw1PBCore#show log
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
   Console logging: level debugging, 3418 messages logged, xml disabled,
                    filtering disabled
   Monitor logging: level debugging, 0 messages logged, xml disabled,
                    filtering disabled
   Buffer logging: level debugging, 3418 messages logged, xml disabled,
                    filtering disabled
   Exception Logging: size (8192 bytes)
   Count and timestamp logging messages: disabled
   Trap logging: level informational, 3422 message lines logged

Log Buffer (4096 bytes):
and port Gi4/4

Sw1PBCore#
Sw1PBCore#!HARDWARE
Sw1PBCore#show version
Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-I9K91S-M), Version
12.2(25)EWA12, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 15-Nov-07 18:28 by kellythw
Image text-base: 0x10000000, data-base: 0x115CC718

ROM: 12.2(31r)SGA1
Dagobah Revision 226, Swamp Revision 34

Sw1PBCore uptime is 9 weeks, 2 days, 2 hours, 19 minutes
Uptime for this control processor is 9 weeks, 2 days, 2 hours, 19 minutes
System returned to ROM by power-on
System image file is "bootflash:cat4000-i9k91s-mz.122-25.EWA12.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

cisco WS-C4507R (MPC8245) processor (revision 10) with 262144K bytes of memory.
Processor board ID FOX1151GEGJ
MPC8245 CPU at 266Mhz, Supervisor II+
Last reset from PowerUp
1 Virtual Ethernet interface
40 Gigabit Ethernet interfaces
511K bytes of non-volatile configuration memory.

Configuration register is 0x2101

Sw1PBCore#show diag
% Incomplete command.

Sw1PBCore#show module
Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

Mod	Ports	Card Type	Model	Serial No.
1	2	Supervisor II+ 1000BaseX (GBIC)	WS-X4013+	JAE11518AXL
2	2	Supervisor II+ 1000BaseX (GBIC)	WS-X4013+	JAE11518AXX
3	24	10/100/1000BaseT (RJ45)	WS-X4424-GB-RJ45	JAE11496C87

```
4    6  SFP, 10/100/1000BaseT (RJ45)V, Cisco/I WS-X4506-GB-T     JAE11528ZC0
5    6  SFP, 10/100/1000BaseT (RJ45)V, Cisco/I WS-X4506-GB-T     JAE11528ZFV

M MAC addresses                Hw  Fw          Sw              Status
--+---------------------------------+---+-----------+---------------+--------
1 001e.7acb.0100 to 001e.7acb.0101 4.5 12.2(31r)SGA 12.2(25)EWA12    Ok
2 001e.7acb.0102 to 001e.7acb.0103 4.5 12.2(31r)SGA 12.2(25)EWA12,   Ok
3 001c.58d2.3478 to 001c.58d2.348f 1.9                          Ok
4 0019.e8dd.02aa to 0019.e8dd.02af 1.4                          Ok
5 0019.e8dd.0310 to 0019.e8dd.0315 1.4                          Ok

Mod  Redundancy role     Redundancy mode     Redundancy status
----+------------------+------------------+------------------
 1   Active Supervisor   SSO                Active
 2   Standby Supervisor  SSO                Standby hot

Sw1PBCore#show inventory
NAME: "Switch System", DESCR: "Cisco Systems, Inc. WS-C4507R 7 slot switch "
PID: WS-C4507R        , VID: V09, SN: FOX1151GEGJ

NAME: "Clock Module", DESCR: "Clock Module"
PID: WS-X4K-CLOCK     , VID: V04, SN: JAE1137WTVQ

NAME: "Mux Buffer 3 ", DESCR: "Mux Buffers for Redundancy Logic"
PID: WS-X4590         , VID: V04, SN: JAE115292BV

NAME: "Mux Buffer 4 ", DESCR: "Mux Buffers for Redundancy Logic"
PID: WS-X4590         , VID: V04, SN: JAE115292KT

NAME: "Mux Buffer 5 ", DESCR: "Mux Buffers for Redundancy Logic"
PID: WS-X4590         , VID: V04, SN: JAE11529291

NAME: "Mux Buffer 6 ", DESCR: "Mux Buffers for Redundancy Logic"
PID: WS-X4590         , VID: V04, SN: JAE115292FZ

NAME: "Mux Buffer 7 ", DESCR: "Mux Buffers for Redundancy Logic"
PID: WS-X4590         , VID: V04, SN: JAE115292FO

NAME: "Linecard(slot 1)", DESCR: "Supervisor II+ with 2 1000BaseX GBIC ports"
```

PID: WS-X4013+ , VID: V14, SN: JAE11518AXL

NAME: "Linecard(slot 2)", DESCR: "Supervisor II+ with 2 1000BaseX GBIC ports"
PID: WS-X4013+ , VID: V14, SN: JAE11518AXX

NAME: "Linecard(slot 3)", DESCR: "10/100/1000BaseT (RJ45) with 48 10/100/1000 baseT ports"
PID: WS-X4424-GB-RJ45 , VID: V05, SN: JAE11496C87

NAME: "Linecard(slot 4)", DESCR: "6 Dual media SFP or 10/100/1000BaseT (RJ45)V voice power ports (Cisco/IEEE)"
PID: WS-X4506-GB-T , VID: V05, SN: JAE11528ZC0

NAME: "GigabitEthernet4/1", DESCR: "1000BaseSX"
PID: SFBR-5766PZ , VID: , SN: AGM114710PT

NAME: "GigabitEthernet4/2", DESCR: "1000BaseSX"
PID: SFBR-5766PZ , VID: , SN: AGM114710PY

NAME: "GigabitEthernet4/3", DESCR: "1000BaseSX"
PID: SFBR-5766PZ , VID: , SN: AGM114710Q3

NAME: "GigabitEthernet4/4", DESCR: "1000BaseSX"
PID: SFBR-5766PZ , VID: , SN: AGM114710PH

NAME: "GigabitEthernet4/5", DESCR: "1000BaseSX"
PID: FTRJ-8519-7D-CSC , VID: , SN: H11F251

NAME: "GigabitEthernet4/6", DESCR: "1000BaseSX"
PID: FTLF8519P2BCL-CS , VID: 00 , SN: FNS11510MLQ

NAME: "Linecard(slot 5)", DESCR: "6 Dual media SFP or 10/100/1000BaseT (RJ45)V voice power ports (Cisco/IEEE)"
PID: WS-X4506-GB-T , VID: V05, SN: JAE11528ZFV

NAME: "GigabitEthernet5/1", DESCR: "1000BaseSX"
PID: SFBR-5766PZ , VID: , SN: AGM114710QC

NAME: "GigabitEthernet5/2", DESCR: "1000BaseSX"

PID: SFBR-5766PZ , VID: , SN: AGM114710RE

NAME: "Fan", DESCR: "FanTray"
PID: WS-X4597 , VID: V08, SN: NWG115003EQ

NAME: "Power Supply 1", DESCR: "Power Supply (AC 1300W)"
PID: PWR-C45-1300ACV , VID: V05, SN: DTH1143N289

NAME: "Power Supply 2", DESCR: "Power Supply (AC 1300W)"
PID: PWR-C45-1300ACV , VID: V05, SN: DTH1143N275

Sw1PBCore#show power

Power Supply	Model No	Type	Fan Status	Inline Sensor	Inline Status
PS1	PWR-C45-1300ACV	AC 1300W	good	good	good
PS2	PWR-C45-1300ACV	AC 1300W	good	good	good

Power supplies needed by system : 1
Power supplies currently available : 2

Power Summary (in Watts)	Used	Maximum Available
System Power (12V)	480	1000
Inline Power (-50V)	0	780
Backplane Power (3.3V)	40	40
Total	520 (not to exceed Total Maximum Available = 1300)	

Sw1PBCore#show redundancy
Redundant System Information :

Available system uptime = 9 weeks, 2 days, 2 hours, 20 minutes
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = none

```
          Hardware Mode = Duplex
  Configured Redundancy Mode = Stateful Switchover
   Operating Redundancy Mode = Stateful Switchover
        Maintenance Mode = Disabled
         Communications = Up

Current Processor Information :
-------------------------------
         Active Location = slot 1
    Current Software state = ACTIVE
   Uptime in current state = 9 weeks, 2 days, 2 hours, 19 minutes
          Image Version = Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-
I9K91S-M), Version 12.2(25)EWA12, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 15-Nov-07 18:28 by kellythw
    Configuration register = 0x2101

Peer Processor Information :
----------------------------
         Standby Location = slot 2
    Current Software state = STANDBY HOT
   Uptime in current state = 9 weeks, 2 days, 2 hours, 20 minutes
          Image Version = Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-
I9K91S-M), Version 12.2(25)EWA12, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 15-Nov-07 18:28 by kelly
    Configuration register = 0x2101


Sw1PBCore#show envi
no alarm

Chassis Temperature              = 34 degrees Celsius
Chassis Over Temperature Threshold    = 75 degrees Celsius
Chassis Critical Temperature Threshold = 95 degrees Celsius
```

Power Supply	Model No	Type	Fan Status	Inline Sensor	Inline Status
PS1	PWR-C45-1300ACV	AC 1300W	good	good	good
PS2	PWR-C45-1300ACV	AC 1300W	good	good	good

Power supplies needed by system : 1
Power supplies currently available : 2

Chassis Type : WS-C4507R

Power consumed by backplane : 40 Watts

Supervisor Led Color : Green

Module 1 Status Led Color : Green
Module 2 Status Led Color : Green
Module 3 Status Led Color : Green
Module 4 Status Led Color : Green PoE Led Color : Green
Module 5 Status Led Color : Green PoE Led Color : Green

ANEXO 2

COMANDOS ROUTER

COMANDOS ROUTER XXXXX

sh version

```
;co Internetwork Operating System Software
S (tm) C806 Software (C806-Y6-M), Version 12.2(2)XI, EARLY DEPLOYMENT RELEASE
FTWARE (fc1)
C Support: http://www.cisco.com/tac
pyright (c) 1986-2001 by cisco Systems, Inc.
mpiled Sat 18-Aug-01 00:56 by ealyon
age text-base: 0x80013170, data-base: 0x804F4010

)M: System Bootstrap, Version 12.2(1r)XE2, RELEASE SOFTWARE (fc1)
)M: C806 Software (C806-Y6-M), Version 12.2(2)XI, EARLY DEPLOYMENT RELEASE SOFT
ARE (fc1)

bertoGilbert uptime is 2 weeks, 2 days, 2 hours, 42 minutes
stem returned to ROM by power-on
stem image file is "flash:c806-y6-mz.122-2.XI.bin"

;CO C806 (MPC855T) processor (revision 0x202) with 14848K/1536K bytes of memor

ocessor board ID JAD05320FJZ (2524829655), with hardware revision 0000
U rev number 5
idging software.
:thernet/IEEE 802.3 interface(s)
8K bytes of non-volatile configuration memory.
92K bytes of processor board System flash (Read/Write)
48K bytes of processor board Web flash (Read/Write)

nfiguration register is 0x2102
```

dir all

```
ectory of nvram:/

24  -rw-     2229          <no date>  startup-config
25  ----        5          <no date>  private-config
1   -rw-        0          <no date>  ifIndex-table

1072 bytes total (127762 bytes free)
ectory of system:/

2  dr-x        0          <no date>  memory
1  -rw-     2229          <no date>  running-config
9  dr-x        0          <no date>  vfiles

space information available
```

```
Directory of flash:/

  1 -rw-   2622084         <no date> c806-y6-mz.122-2.XI.bin
  2 -rw-      1187         <no date> no

8388608 bytes total (5765208 bytes free)
Directory of webflash:/

  1 -rw-      3379         <no date> home.html
  2 -rw-     24396         <no date> GUI.html
  3 -rw-      8082         <no date> loading.gif
  4 -rw-    398691         <no date> CRWS_1.jar
  5 -rw-    134152         <no date> CRWS_2.jar
  6 -rw-       881         <no date> ConfigExp.cfg

2097152 bytes total (1527180 bytes free)
```

- **sh run**

```
Building configuration...

Current configuration : 2229 bytes
!
version 12.2
no parser cache
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname RobertoGilbert
!
logging rate-limit console 10 except errors
enable secret 5 $1$GCWF$6e2kCWZNjlJv9z3yYMdli/
enable password 7 060506324F41
!
username Cisco privilege 15 password 7 00404242330A0D274B2E1D413A3C15161A221B221
C0D153B31022C
username administrador privilege 15 password 7 094D4A044A5542000C
clock timezone GMT -5
ip subnet-zero
no ip domain-lookup
ip host maternidad xxx.xxx.xxx.xxx
ip host juntamatriz xxx.xxx.xxx.xxx
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
!
!
interface Ethernet0
```

```
 ip address xxx.xxx.xxx.xxx 255.255.255.0
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address xxx.xxx.xxx.xxx 255.255.255.0
 no cdp enable
!
ip default-gateway xxx.xxx.xxx.xxx
ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip route xxx.xxx.xxx.xxx  0.0.0.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx
ip route xxx.xxx.xxx.0 255.255.255.0 xxx.xxx.xxx.xxx name CONT
ip route xxx.xxx.xxx.0 255.255.0.0 xxx.xxx.xxx.xxx
ip http server
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
snmp-server community public RO
snmp-server location Hospital
banner login ^C
**************************************************
*                                                *
*        HOSPITAL  XXXXX        *
*                               *
*          - XXXXXXX -          *
*  ACCESOS NO AUTORIZADOS ESTAN PROHIBIDOS  *
*          Y SERAN REPORTADOS!!!          *
**************************************************
^C
!
line con 0
 exec-timeout 120 0
 logging synchronous
 login local
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 121A0C041104
 login local
 length 0
 transport input telnet
!
```

scheduler max-task-time 5000
end

- **sh ip route**

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

Gateway of last resort is xxx.xxx.xxx.xxx to network 0.0.0.0

S   xxx.xxx.xxx.xxx/16 [1/0] via xxx.xxx.xxx.xxx
    xxx.xxx.0.0/16 is variably subnetted, 10 subnets, 2 masks
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
S     xxx.xxx.xxx.0/24 [1/0] via xxx.xxx.xxx.xxx
C     xxx.xxx.xxx.0/24 is directly connected, Ethernet0
S     xxx.xxx.xxx.0/24[1/0] via xxx.xxx.xxx1
C   xxx.xxx.xxx.0/24 is directly connected, Ethernet1
S*  0.0.0.0/0 [1/0] via xxx.xxx.xxx.xxx
```

- **sh ip interface brief**

```
Interface          IP-Address     OK? Method Status            Prot
ocol
Ethernet0          xxx.xxx.20.5   YES NVRAM  up               up

Ethernet1          xxx.xxx.xxx3     YES NVRAM  up               up
```

- **sh cdp neighbors**

% CDP is not enabled

- **sh logging**

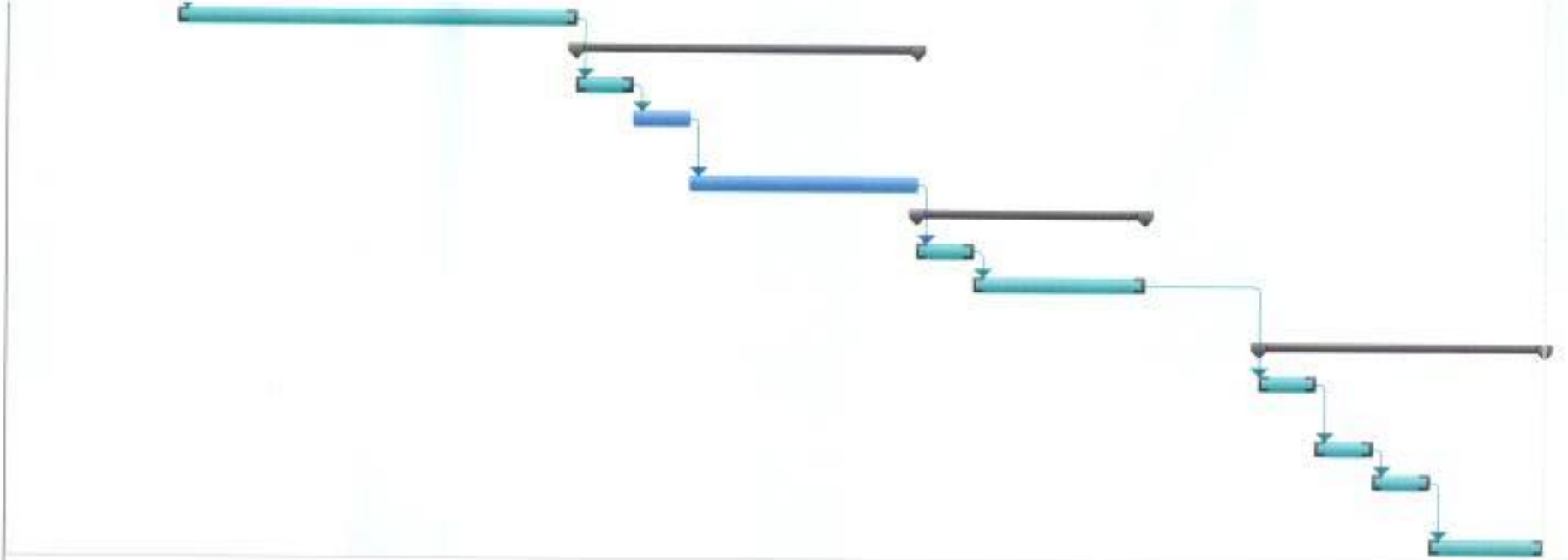
```
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes,
0 overruns)
   Console logging: level debugging, 7 messages logged
   Monitor logging: level debugging, 0 messages logged
   Buffer logging: level debugging, 7 messages logged
   Logging Exception size (2048 bytes)
   Trap logging: level informational, 12 message lines logged

Log Buffer (2048 bytes):
```

ANEXO 3

4		LEVANTAMIENTO DE INFORMACIÓN WAN	5 días	mié 24/10/12 mar 30/10/12
5		**IMPLEMENTACIÓN RED LAN**	**4 días**	**mié 31/10/12 lun 05/11/12**
6		ACTUALIZACIÓN DE IOS EN SWITCH DE NUCLEO	1 día	mié 31/10/12 mié 31/10/12
7		INSTALACIÓN DE TARJETAS EN CONMUTADOR DE NUCLEO	1 día	jue 01/11/12 jue 01/11/12
8		INSTALACIÓN DE ENLACE DE REDUNDANCIA	2 días	vie 02/11/12 lun 05/11/12
9		**IMPLEMENTACIÓN RED WAN**	**4 días?**	**mar 06/11/12 vie 09/11/12**
10		INSTALACIÓN DE ENRUTADOR WAN	1 día?	mar 06/11/12 mar 06/11/12
11		CONFIGURACIÓN DE PROTOCOLO DE ENRUTAMIENTO DINÁMICO	3 días	mié 07/11/12 vie 09/11/12
12		**IMPLEMENTACION DE MONITOREO Y GESTION**	**5 días**	**lun 12/11/12 vie 16/11/12**
13		INSTALACION DEL SERVIDOR, SISTEMA OPERATIVO Y PARCHES	1 día	lun 12/11/12 lun 12/11/12
14		INSTALACION DE CISCO LMS	1 día	mar 13/11/12 mar 13/11/12
15		AGREGACION DE DISPOSITIVOS AL SISTEMA DE MONITOREO	1 día	mié 14/11/12 mié 14/11/12
16		CONFIGURACION DE SNMP	2 días	jue 15/11/12 vie 16/11/12

Proyecto: Proyecto1
Fecha: mié 17/10/12

Tarea		Resumen inactivo	
División		Tarea manual	
Hito		Sólo duración	
Resumen		Informe de resumen manual	
Resumen del proyecto		Resumen manual	
Tareas externas		Sólo el comienzo	
Hito externo		Sólo fin	
Tarea inactiva		Fecha límite	
Hito inactivo		Progreso	



Proyecto: Proyecto1
Fecha: mié 17/10/12

Tarea		Resumen inactivo	
División		Tarea manual	
Hito		Sólo duración	
Resumen		Informe de resumen manual	
Resumen del proyecto		Resumen manual	
Tareas externas		Sólo el comienzo	
Hito externo		Sólo fin	
Tarea inactiva		Fecha límite	
Hito inactivo		Progreso	