PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

ESTUDIO DE UN MODELO DE SEGURIDAD DE LA INFORMACION QUE SEA APLICABLE A INSTITUCIONES DE LA SALUD. CASO DE ESTUDIO HOSPITAL DR. JULIO VILLACRESES COLMONT DE LA CIUDAD DE PORTOVIEJO.

RAÚL SOLÓRZANO

Quito – 2016

INDICE

INDICE DE FIGURAS:

INDICE DE TABLAS:

1 INTRODUCCIÓN

El presente proyecto de estudio cubre la reestructuración de las redes de datos del hospital “Dr. Julio Villacreses Colmont” de la ciudad de Portoviejo.

En la actualidad, las organizaciones hacen uso de las tecnologías de información y comunicaciones para ayudar al desarrollo de sus procesos y lograr sus objetivos. Por esta razón se requiere una infraestructura de redes que cumpla con los requerimientos de las tendencias modernas, convergencia de servicios y recursos de la actualidad; proyectándose a mediano plazo.

Para proponer una estructura de red acorde a las tendencias, es necesario realizar un análisis actual del sistema de cableado, los dispositivos activos, la conectividad interna y de internet, las necesidades actuales de información, la comunicación de servicios adicionales que requiere dicha institución, teniendo en cuenta también la factibilidad de expansión de tecnologías a medida que pase el tiempo y la demanda de más servicios se presente.

Cada área requiere de métodos y basados en estándares de operación tecnológica y seguridad respecto a comunicación de datos, lo que implica realizar estudios de factibilidad para aplicar sistemas que permitan facilitar el control y manejo de la información en los servicios a realizar con los pacientes, es ahí cuando interactúan los profesionales unidos en la misma meta, que es de proporcionar calidad de servicio, seguridad e integridad.

2 JUSTIFICACION

Como es de poco conocimiento, en los actuales tiempos interacción entre personal profesional médico y personal profesional de tecnologías en la mayoría de los casos están llevando bajo protocolo de comunicación simple no estandarizado correspondiente a normas de estandarización y seguridad, se ha visto y notado en muchas ocasiones malestares con base a problemas de interrupciones que surgen en la red de datos, a consecuencia de ello el tiempo de espera superan en algunas veces en minutos perjudicando administrativamente la productividad del personal, al mismo tiempo atrasando las actividades que son planificadas en un orden especifico mientras se dan las actividades. A demás la integridad y seguridad de la información que fluye en la red se ve amenazada por tales falencias o vulnerabilidades.

La variante en ciertos horarios de atención cuando el volumen de tráfico de la red aumenta considerablemente complicando labores de procesamiento de archivos y transacciones, depende de la fluidez en que circulan los paquetes de datos. Como meta de este trabajo implica optimizar el uso de las redes hospitalarias cumpliendo con las normas de tecnologías establecidas, aportando a que a través de las estaciones de trabajo, dispositivos activos e infraestructura interna de datos de la entidad, operen de la mejor manera reduciendo los inconvenientes que se puedan presentar y sobre todo protegiendo la información que es motivo principal de este documento.

3 ANTECEDENTES

Tomando en cuenta que en esta institución lleva muchos años brindando sus servicios a muchos pacientes y sobre todo a casos especializados como es la oncología, implica que ha tenido que sobrellevar la información de criterio confidencial a tomar en cuenta tecnologías como el uso de sistemas hospitalarios como herramienta para sobrellevar las labores diarias. Esto ha permitido la expansión de sus servicios y el incremento en el almacenamiento de la información que es muy esencial e importante.

La incorporación de mecanismos de almacenamiento y la infraestructura de red de datos en los actuales momentos ha pasado a ser considerada para mejoramiento y más aún para incorporar sistemas de seguridad que ayuden a proteger y resguardar la información, de lo que actuales momentos no lo posee.

Es por ello que el fin de este trabajo el aportar a una solución de reestructurar las redes de comunicaciones que son de vital relevancia para lograr el objetivo que exige la garantía de la información. El estudio de este esquema pretende explicar una manera adecuada de llevar implementaciones de sistemas de red para ambientes hospitalarios. Las aplicaciones a estas referencias están basadas en normas a seguir rigurosamente y dependerá de las dimensiones en áreas geográficas el tamaño del proyecto para el cual fuese a desarrollarse.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Estudiar diferentes alternativas que permitan seleccionar un modelo de seguridad de la información que sea aplicable a instituciones hospitalarias. Caso de estudio hospital Dr. Julio Villacreses Colmont de la ciudad de Portoviejo.

4.2 OBJETIVOS ESPECÍFICOS

1. Definir los modelos de seguridad de información e identificar uno que permita desarrollar una solución que optimize el esquema en producción para consideraciones elementales de alto rendimiento.

2. Analizar la situación actual de la infraestructura de red del hospital para reestructurar la red de datos.

3. Diagnosticar el estado del tráfico de la red para el establecimiento sobre la situación presente.

4. Describir las topologías para aplicar un escenario de redundancia y modelo de seguridad.

5. Validar el planteamiento del nuevo esquema de optimización de la infraestructura por expertos.

5 DESARROLLO CASO DE ESTUDIO

5.1 DEFINICION DE MODELOS DE SEGURIDAD

La terminología de seguridad de la información refiere en aspectos de protección de la confidencialidad, integridad y disponibilidad de la información. Debido a estos aspectos se considera tratar esta temática por niveles debido a que pasa por diferentes capas para establecer comunicación entre dos o más estaciones de trabajo. La seguridad de la información puede implementarse por niveles tomando los niveles de la referencia del modelo OSI.

5.1.1 MODELO DE SEGURIDAD EN LA CAPA FISICA

Tomando en cuenta la seguridad física no debe llevarnos a gastos excesivos, lo primordial es focalizar los sitios claves y apuntar nuestra atención, ***"luego de ello lanzar toda la información lo más claramente posible y posteriormente pasar a formar parte de un sistema de gestión de seguridad de la información SGSI."*** (seguridad, 2012)

En el modelo TCP/IP la capa de acceso a la red que corresponde a la capa 1 y 2 del modelo referencial OSI, se ocupa de todos los aspectos que conlleven a convertir un paquete en una trama y transmitirlo a través de un medio físico. (seguridad, 2012)

5.1.1.1 ASPECTOS FISICOS

- ***"Lo propio o lo arrendado: lo propio pasa exclusivamente por vías de acceso no público, esto incrementa la seguridad de interceptación. Por otro lado lo arrendado se debe tomar en cuenta que si se puede ser interceptado; para ello existen estrategias de canalización segura, túneles o criptografía que aporta a la seguridad.***

- ***Material de cobre: Este medio presenta la característica que es difícil detectar su interceptación física o pinchada en línea.***

- ***Fibra Optica: Esta se puede considerar difícil de interceptar, ya que existen divisores ópticos en sus extremos y entre segmentos, incorporar más de los mismos implica un corte en el canal y una fácil detección por perdida de potencia óptica.***

- ***Laser: Este medio genera un haz de luz lineal apuntando a un receptor, el cual es el único punto que impacta la señal, si bien es interceptable, es similar a la fibra se detecta con facilidad.***

- ***Infrarrojo: Se implementa de dos maneras, por alcance directo y por reflexión, el primero se emplea para distancia muy cortas y el segundo se refleja en paredes llegando parte de esta señal al receptor, por lo que es vulnerable.***

- ***Radiofrecuencia: Las ondas de radio cubren una amplia gama de posibilidades, desde las altas frecuencias hasta las microondas, son interceptables.***

En cada uno de los mencionados implica una modalidad diferente en su auditoria tomando como punto de partida lo siguiente:

- ***Identificación de los canales: Aquí debe ir indicado claramente su numeración, puestos de trabajo y extremos.***

- ***Gabinetes de comunicación: Tiene que ver con la ubicación, llaves, seguridad de acceso, identificador de boquillas.***

- ***Caminos a seguir: Planos del establecimiento perfectamente identificados los ductos por colores.***

- ***Dispositivos de Hardware de red: La cantidad de dispositivos existentes, localización física, claves de acceso, resguardo de las configuraciones, habitaciones, habilitación y deshabilitación de puertos.***

- ***Dispositivos mecánicos u ópticos para control de acceso: Control por tarjetas, biométricos, dactilares.***

- ***Certificación de medios: Normas establecidas TIA/EIA, TSB-67***

- ***Control de cambios: Cualquier modificación que se presente en la red debe quedar documentada.***

- ***Inventario de equipamiento: Llevar el control de inventario en especial los equipos que llevan la información almacenada.***

- ***Medidas de resguardo de la información: La pérdida de información en servidores es un grave error, el encargado de las bases de datos debe mantener todos los mecanismos de backup en los diferentes medios posibles."*** (seguridad, 2012)

5.1.1.2 ASPECTOS LOGICOS

- ***"Análisis de la topología de red: Muy importante ya que mantendrá una lógica de la información.***

- ***Estrategias de expansión: El crecimiento de una red es uno de los primeros argumentos de diseño, una LAN bien diseñada responderá a un crecimiento lógico adecuado.***

- ***Consideración de prioridades y reservas de acceso a la red: En las redes 802.4, 802.5 y 802.11 se llevan a cabo con total cuidado y permite regular el acceso a los recursos.***

- ***Lógica empleada en VPN: Es una capacidad que ofrecen actualmente los dispositivos activos de la red, se configuran los puertos formando grupos independientes.***

- ***Análisis de circuitos y caminos: Va más orientada a las redes WAN, se programan las conexiones previamente para que controlar que nada quede fuera de lo permitido.***

- ***Puntos de acceso a la red: Auditar correctamente que esté documentado y que cada uno de los accesos a la red sea estrictamente necesaria, en especial a las redes inalámbricas.***

- ***Potencia eléctrica u óptica: La irradiación de toda señal electromagnética implica ser tomado en cuenta, cuanto menor sea la potencia, se reduce el radio de propagación, es un detalle que es relevante para medios de transmisión como antenas o fibras ópticas.***

- ***Rango de frecuencias empleadas: Se debe especificar la cantidad de canales que se emplean y su tipo de configuración. (análogo, digital, simplex dúplex, semiduplex, E1, etc...)***

- ***Planos de distribución de emisores y receptores: Se debe aclarar su ubicación física, características técnicas, alcance y medidas de protección.***

- ***Ruido y distorsión en líneas: Este elemento causa perdida de información y facilita la posibilidad de ataques."*** (seguridad, 2012)

5.1.2 MODELO DE SEGURIDAD EN LA CAPA DE ENLACE

En lo que respecta a protocolos de comunicación que operan a nivel de capa de enlace, existen varios pero exclusivamente se concentrará en dos más importantes que son 802.3 y 802.11. Al igual que con la capa física, existen vulnerabilidades de esta capa que están allegadas al medio sobre el que se realiza la conexión y transmisión de datos. Este nivel comprende la conexión con el modo inmediatamente adyacente, lo que en una red punto a punto es perfectamente claro, pero en una red LAN, es complicado determinar cuál es el nodo adyacente. Es por ello que se menciona en la teoría IEEE en dos subniveles: LLC y MAC.

La importancia de este nivel, es que es el último que encapsula todos los anteriores, por lo tanto si se escucha y se sabe desencapsular se tiene acceso a toda la información que circula en la red. Las herramientas que operan a este nivel de capa son los analizadores de protocolos conocidos y que son de diferentes tipos. (seguridad, 2012)

Para llevar un mejor control de deben tomar en cuenta ciertas consideraciones:

- ***"Control de direcciones de hardware: Poseer el control de la totalidad de las direcciones de hardware de la red, esto involucra tener la lista de direccionamiento MAC o conocida también como NIC.***

- ***Control de configuración de switches: Estos son los dispositivos que operan a nivel de capa 2, su labor consiste en ir aprendiendo porque puerto se hace presente una dirección MAC, a medida que va aprendiendo, conmuta el tráfico por la puerta adecuada, segmentando la red en diferentes dominios de colisión.***

- ***Análisis de tráfico: En este punto la transmisión puede ser unicast, multicast o broadcast. El rendimiento de una red se ve afectado con la presencia de broadcast, de hecho una de las medidas para optimizar redes y motivo de ataques conocidos como bombardeo de broadcast. En otro tipo de medida es el análisis de multicast ya que estos mensajes se intercambian entre dispositivos routers, es de sumo provecho para interesados en una red ajena ser partícipes, pues ahí se encontrará toda la información servida sobre el ruteo de la red.***

- ***Análisis de colisiones: Cuando un host transmite y otro en un intervalo de tiempo menos a 512 microsegundos, si se encuentra a una distancia tal que la señal del primero no llegó, se le ocurre transmitir también. Este hecho, los dos host hacen silencio y esperan una cantidad aleatoria de tiempo de ranura, es decir, 512 microsegundos, e intentan transmitir nuevamente. Si se tiene acceso físico a la red, un ataque de negación de servicios DoS, es justamente generar colisiones ya que obliga a hacer silencio a todos los host de ese segmento.***

- ***Evaluación de puntos de acceso inalámbrico: Este tipo de tecnología es segura si se configura adecuadamente, por tal motivo hay que verificar que tipo de protocolos de autenticación se han considerado, los permisos de accesos a estos dispositivos, su potencia de emisión, etc…"*** (seguridad, 2012)

5.1.3 MODELO DE SEGURIDAD EN LA CAPA DE RED

"La funcionalidad relevante de esta capa es el manejo de las rutas, se baja en el protocolo IP que es de nivel 3 no encaminado a la conexión, permitiendo el intercambio de datos sin el establecimiento previo de la llamada. Una característica esencial es que soporta operaciones de fragmentación y desfragmentación, por lo cual un datagrama se subdivide y segmenta en paquetes más pequeños para ser introducidos a la red, posterior a ello en el destino se reconstruyen en su formato original para entregarlos al nivel superior. La otra operación que tiene importancia se trata del ruteo, el cual incorpora por medio de un esquema de direccionamiento.

Un atacante puede suplantar un paquete si indica que proviene de otro sistema, la suplantación se puede dar por ejemplo, al dar una repuesta a otro mensaje antes de que lo haga el suplantado.

En esta capa la autenticación de los paquetes se realiza a nivel de máquina, es decir, dirección IP, y no a nivel de usuario. Por lo que si un sistema suministra una dirección de máquina errónea, el receptor no detectará la suplantación. Para conseguir el objetivo, este tipo de ataques suele utilizar técnicas, como la predicción de números de secuencia TCP, envenenamiento de tablas cache, etc… También se pueden manipular los paquetes si se modifican sus datos y se reconstruyen de forma adecuada los controles de cabecera, todo esto, el receptor es incapaz de detectar el cambio." (seguridad, 2012)

5.1.3.1 CONSIDERACIONES DE AUDITORIA EN ROUTERS

"Para ello se deberá llevar ciertos niveles de auditorías en los dispositivos de capa 3 como son:

- ***Control de contraseñas: Los dispositivo routers permiten la configuración de distintos tipos de contraseña, para acceder al modo usuario es la que primero solicita vía telnet, luego también para el ingreso en modo privilegiado, permite además el acceso a una contraseña cifrada, la de acceso por vía consola y por interfaz gráfica http.***

- ***Configuración de routers: En este aspecto se contempla detalles de configuración que normalmente quedan muchas ocasiones quedan habilitados innecesariamente.***

- ***Resguardo de las configuraciones: Una importancia de este punto es de almacenar la configuración startupconfig, en forma consistente con la running-config y al mismo modo en un servidor ftp y de ser posible documentada también.***

- ***Protocolos de ruteo: El empleo de estos es crítico pues la mayor flexibilidad está dada por el uso de (RIP, IGRP, EIGRP, OSPF), pero hay que tener en cuenta que con esta medida se facilita información para ser aprovechada por intrusos, los cuales pueden utilizarla para participar de las tablas de ruteo. Las tablas de ruteo estáticas, por lo contrario, aumentan sensiblemente las medidas de seguridad, ya que toda ruta que no esté contemplada, no podrá ser alcanzada.***

- ***Listas de control de acceso: Son las primordiales en el acceso de la red.***

- ***Listas de acceso extendidas: Además de incorporar las funciones descritas anteriormente, estas las amplían con parámetros de nivel de transporte.***

- ***Seguridad de acceso por consola: El acceso por consola viene por defecto habilitado sin ninguna restricción, y si se tiene acceso físico a dispositivo routers, se puede obtener el control del mismo. Un usuario experto puede iniciar la secuencia de recuperación de contraseña para reemplazar por una nueva.***

- ***Mejor ruta: Esta trata de un mensaje tipo ICMP, su mal uso permite perfilar la ruta de una red para obligarla a pasar siempre por un router sobre el cual se obtiene información deseada.***

- ***Solicitud y respuesta: Se determina por un protocolo ICMP con una solicitud y respuesta eco, tal cual conocido como el ping, Un conocido ataque es enviarlo con una longitud mayor a lo permitido por IP (65535) bytes. Al recibirse el host no sabe cómo tratarlo y se bloquea.***

- ***Auditoria ARP: Es uno de los más complejos de detectar pues se refiere a la asociación incorrecta de direcciones MAC o IP, por lo tanto se tiene que analizar todas las tramas que circulan por la red y compararlas frecuentemente con un patrón de referencia valido."*** (seguridad, 2012)

5.1.4 MODELO DE SEGURIDAD EN LA CAPA DE TRANSPORTE

Esta capa se encarga de la calidad de servicio, dando garantía a cuando la aplicación lo requiera de proporcionar confiabilidad, control de flujo, segmentación y control de errores. Está basado en los protocolos TCP y UDP específicamente y lo hace sobre datagramas IP. Aquí se pueden encontrar inconvenientes de autenticación, de integridad y confidencialidad. Algunos ataques conocidos en esta capa son las de denegación de servicios por protocolos de transporte.

En este nivel dentro de TCP/IP como se había mencionado anteriormente, existirán dos posibilidades, operar en modo orientado a la conexión lo cual se emplea TCP o sin conexión cuyo protocolo es UDP, el responsable de decidir que protocolo entregará el mensaje es el que se emplee en el nivel superior, para lo cual existe el concepto de puerto SAP entre el nivel de transporte y el de aplicación. (seguridad, 2012)

5.1.4.1 AUDITORIA EN UDP

Este Protocolo por no ser orientado a la conexión, no implementa ninguno de los bits de TCP, por lo tanto es difícil regular su ingreso o egreso en una red. Mientras un proxy, solo puede regular las sesiones TCP. A diferencia de un firewall es que el último puede contener las asociaciones entre los segmentos UDP y el datagrama correspondiente, de esa firma puede filtrar toda asociación inconsistente. Este tipo de firewall son los que permiten un filtrado dinámico de paquetes y como medida de precaución cierra todos los puertos UDP que no se necesiten. (seguridad, 2012)

5.1.4.2 AUDITORIA DE PUERTOS UDP Y TCP

En el encabezado de TCP o UDP se encuentran los campos puerto de origen y destino, los cuales son uno de los detalles más importantes a auditar de una red, por medio de ellos se puede ingresar a un host y operar dentro de este. Por lo que se deberá considerar las medidas en adoptar acorde a los puertos detallados en el nivel de transporte al análisis de puertos. (seguridad, 2012)

5.1.5 MODELO DE SEGURIDAD EN LA CAPA DE APLICACIÓN

Cuando ya se ha pasado el cuatro que es transporte, las funciones y servicios se orientan al usuario, a partir de este nivel es poco probable que se encuentren observaciones respecto a la red, lo que enfocaremos a lo que el modelo TCP engloba aplicación lo que trata como tres capas el modelo OSI. El modelo TCP/IP combina los aspectos de las aplicaciones en donde se definen los protocolos de alto nivel, estos son de representación y codificación de los datos y control entre los procesos. Esta capa presenta algunas deficiencias de seguridad asociadas a sus protocolos. Debido al gran número de protocolos de esta capa, la cantidad de vulnerabilidades sería superior al de las demás capas. (seguridad, 2012)

5.1.5.1 SERVIDORES DE CORREO, FTP, WEB Y PROXY

- ***"Limitar el acceso en áreas específicas de estos servidores.***

- ***Detallar una lista de grupos y usuarios con sus permisos correspondientes.***
- ***Mantener la utilización de contraseñas seguras***
- ***Mantener un control de los archivos log.***
- ***Deshabilitar los servicios de red que no sean empleados por el servidor.***
- ***Deshabilitar índices de los repositorios."*** (seguridad, 2012)

5.1.5.2 ACCESOS REMOTOS

Es muy común en los actuales momentos que se tenga que trabajar fuera de la empresa, lo cual es una buena medida permitir el acceso remoto mediante líneas fijas o por dispositivos móviles. El primer concepto que se debe tener en cuenta es implementar un pool en el Access server con una única puerta de acceso, lo segundo seria estar permanentemente controlándola con alternativas de autenticación y autorización sobre ciertos accesos. Un firewall es un sistema indicado de defensa ubicado entre la red que se desea asegurar y el exterior, por lo tanto todo tráfico de entrada o salida debe pasar obligatoriamente por esta barrera de seguridad. (seguridad, 2012)

5.1.6 IDENTIFICACIÓN DE UN ESQUEMA QUE PERMITA LA OPTIMIZACIÓN DEL SISTEMA ACTUAL EN PRODUCCIÓN.

Habiendo tenido en cuenta el análisis de la infraestructura de la red, se debe elaborar un análisis de factibilidad que permita un entendimiento claro de todas las necesidades técnicas que se requieren para dimensionar el diseño de implementación a una red convergente, así como el cumplimiento de los servicios actuales y nuevos que se deseen implementar a futuro en la plataforma tecnológica, sin descuidar las debilidades y amenazas en cuanto a seguridad de la información.

La nueva red convergente deberá soportar varios servicios de alto rendimiento en la LAN, servicios de video conferencia, video vigilancia y telefonía IP. La nueva red se deberá especificar en cuanto a:

a) Medios de transmisión o enlaces de comunicación
b) Sistema de cableado estructurado
c) Equipamiento para nuevo backbone y redes en base a modelo de capas
d) Niveles de seguridad recomendados con base a modelo e capas
e) Establecer y definir servicios, características y equipamiento para telefonía IP, video conferencia y video vigilancia

De igual manera se establecerán criterios para seleccionar la mejor propuesta, por factibilidad tecnológica, desempeño y seguridad, que permitan al departamento de informática de la institución, seleccionar la tecnología más adecuada a los fines que se determinen como parte del estudio.

5.1.6.1 ASPECTOS GENERALES DEL DISEÑO

"Las computadoras y las redes de información son esenciales para lograr el éxito en organizaciones grandes o pequeñas. Estas conectan a las personas, admiten aplicaciones, servicios y proporcionan acceso a los recursos que mantienen el funcionamiento de las instituciones. Para cumplir con los requisitos diarios de las empresas, las redes se están volviendo complejas.

Actualmente la economía basada en internet a menudo demanda un servicio al cliente las 24 horas. Lo que significa que las redes comerciales deben estar disponibles casi al 100% del tiempo. Deben ser suficientemente inteligentes como para protegerse automáticamente de los incidentes de seguridad

imprevistos. Deben además adaptarse a las cargas de tráfico cambiantes para mantener tiempos de respuesta constantes en las aplicaciones.

En general, los usuarios de la red no piensan en términos de complejidad de la red subyacente, consideran la red como forma de acceder a las aplicaciones que necesitan." (Cisco Systems, 2007)

5.1.6.2 REQUISITOS QUE DEBE CUMPLIR LA RED

"En la mayoría de las organizaciones solo incluye algunos requisitos para sus redes:

- ***La red debe estar activa a toda hora, incluso en caso de falla en los enlaces, en el equipo y en condiciones de sobrecarga.***
- ***Debe entregar aplicaciones de manera confiable y proporcionar tiempos de respuesta razonables de host a host.***
- ***Se debe proteger los datos que se transmiten a través de la misma, al igual que los datos almacenados en los dispositivos que se conectan a ella.***
- ***La red debe ser fácil de modificar para adaptarse al crecimiento de la red y a los cambios generales de la institución.***
- ***La resolución de problemas debe ser sencilla, ya que las fallas ocurren con frecuencia; la detección y resolución de un problema no debe llevar demasiado tiempo.***

En lo que respecta a los objetivos fundamentales del diseño, se resumen cuatro puntos: Escalabilidad, Disponibilidad, Seguridad y Facilidad de administración." (Cisco Systems, 2007)

5.1.6.3 DISEÑO JERÁRQUICO

"Las arquitecturas empresariales de redes de datos pueden utilizarse para dividir aún más el diseño jerárquico en tres capas en áreas modulares. Los módulos representan áreas que tienen una conectividad física y lógica diferente. Se encargan de designar donde se llevan a cabo las diferentes funciones de la red.

Esta modalidad permite flexibilidad en el diseño de la red, facilita la implementación y la resolución de problemas; estas tres áreas de enfoque de diseño modular de red son:" (Cisco Systems, 2007)

5.1.6.4 CAMPUS EMPRESARIAL

"Donde contiene los elementos de red que se requieren para una operación independiente dentro de un solo campus permitiendo describir los métodos escalables de una red y obtener datos e información según las necesidades de la institución." (Cisco Systems, 2007)

5.1.6.5 GRANJA DE SERVIDORES

"La granja de servidores del centro de datos protege los recursos del servidor y proporciona una conectividad de alta velocidad redundante y confiable." (Cisco Systems, 2007)

5.1.6.6 MARGEN EMPRESARIAL

"A medida que el tráfico ingresa a la red del campus, este segmento filtra el tráfico de los recursos externos y los direcciona hacia la red institucional, contiene todos los elementos requeridos para lograr una comunicación eficiente, segura, las comunicaciones remotas, internet." (Cisco Systems, 2007)

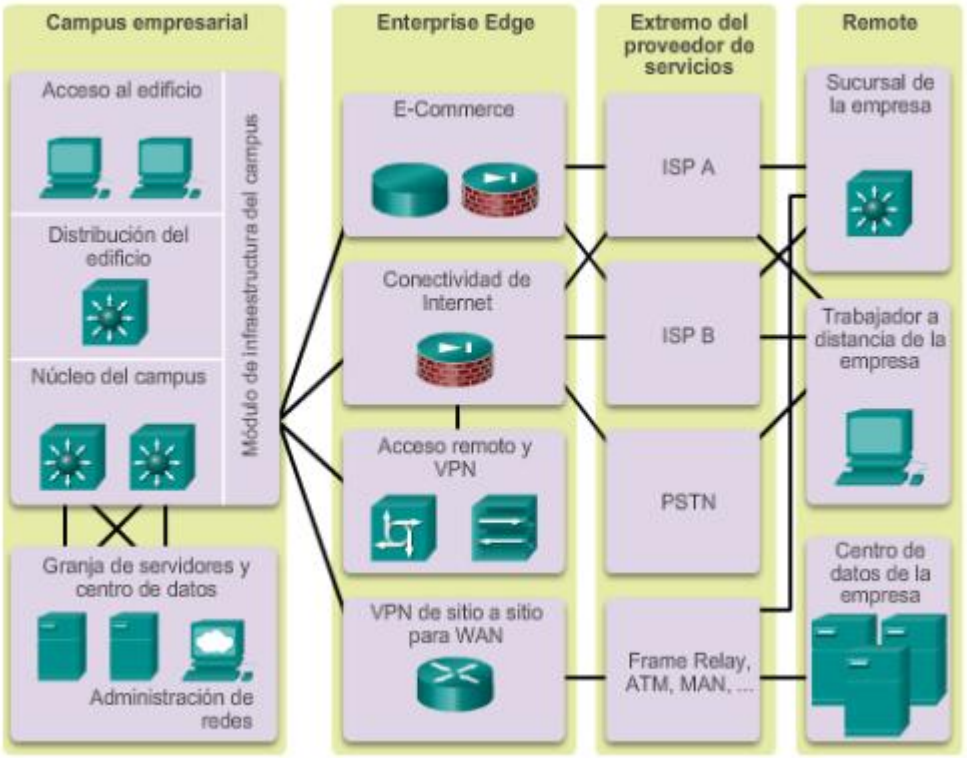


Fig. 1.- Diseño jerárquico
Fuente: Referencia [1]

5.1.7 BENEFICIOS DEL MODELO JERÁRQUICO

- ***"Crea una red determinista con límites claramente definidos entre los módulos. Esto provee puntos claros de demarcación para determinar exactamente en donde se origina el tráfico y donde fluye.***
- ***Facilita la tarea de diseño e implementación al lograr que cada módulo sea independiente.***
- ***Proporciona escalabilidad al permitir a la institución agregar módulos fácilmente, a medida que aumenta la complejidad de la red, se puede agregar nuevos módulos funcionales.***
- ***Permite agregar servicios y soluciones sin cambiar de diseño de la red subyacente."*** (Cisco Systems, 2007)

5.1.8 LA CAPA DE NÚCLEO DE LA RED

"La capa de núcleo se denomina backbone de la red. Los dispositivos switches en la capa de núcleo proporcionan conectividad de alta velocidad. En una LAN institucional, la capa de núcleo puede conectar múltiples edificios o sitios, además proporcionar conectividad a la granja de servidores, incluye uno o más enlaces a los dispositivos en el margen a fin de admitir internet, redes virtuales (VPN), intranet y acceso a WAN. La implementación de un a capa de núcleo reduce la complejidad de la red, lo cual facilita la administración y resolución de problemas." (Cisco Systems, 2007)

5.1.9 OBJETIVOS DE LA CAPA DE NÚCLEO

"El diseño de la capa de núcleo permite la transferencia de datos eficiente y de alta velocidad entre una y otra sección de la red. Los objetivos principales del diseño en la capa de núcleo son:

- ***Proporcionar una capacidad máxima de tiempo de conectividad***
- ***Maximizar el rendimiento***
- ***Facilitar el crecimiento de la red"*** (Cisco Systems, 2007)

5.1.10 ENLACES REDUNDANTES

"La implementación de enlaces redundantes en la capa de núcleo garantiza que los dispositivos de red puedan encontrar caminos alternativos para enviar datos en caso de fallas. Cuando los dispositivos de la capa 3 se colocan en la capa de núcleo, estos enlaces redundantes pueden utilizarse para realizar el balanceo de carga, además de proporcionar respaldo.

En un diseño de red plana de capa 2, el protocolo Spanning Tree (STP) deshabilita los enlaces redundantes, a menos que falle un enlace principal. Este comportamiento del STP previene el balanceo de carga sobre los enlaces redundantes." (Cisco Systems, 2007)

5.1.11 TOPOLOGÍA MALLA

"La mayoría de las capa núcleo de una red se conectan en una topología de malla completa o malla parcial. Una topología de malla completa es donde cada dispositivo posee una conexión con los demás dispositivos. Si bien las topologías de malla completa proporcionan la ventaja de una red completamente redundante, estas pueden ser difíciles de conectar y administrar. Para las instalaciones más grandes, se utiliza un a topología malla parcial modificada. En una topología de malla parcial, cada dispositivo se conecta al menos a otros dos dispositivos, lo cual crea una redundancia suficiente sin la complejidad de una malla completa." (Cisco Systems, 2007)

5.1.12 REDUCCIÓN DEL ERROR HUMANO

"Los errores humanos contribuyen a las fallas en la red, lamentablemente, estos factores no pueden eliminarse al agregar equipos y enlace redundante; muchas fallas de la red son resultado de las actualizaciones o adiciones mal planificadas y sin probar al nuevo equipo.

Las fallas en la capa de núcleo provocan interrupciones generalizadas, es esencial contar con procedimientos y políticas adecuadas por escrito para determinar de qué manera se deben autorizar, probar, aplicar y documentar los cambios. Se debe planificar una estrategia de retirada para regresar la red a su estado anterior si los cambios no producen el resultado esperado. " (Cisco Systems, 2007)

5.1.13 LA CAPA DE DISTRIBUCIÓN

"Esta capa representa un límite de enrutamiento entre la capa de acceso y la capa núcleo. También sirve como punto de conexión entre los sitios remotos y capa núcleo.

La capa de acceso comúnmente se crea utilizando una tecnología de conmutación de capa 2, la capa de distribución se crea utilizando dispositivos de capa 3. Los Routers y Switches multicapa, ubicados en la capa de distribución, proporcionan muchas funcionalidades que son esenciales para cumplir con los objetivos del diseño de red, los cuales son:

- ***Filtrar y administrar los flujos de trafico***
- ***Exigir el cumplimiento de las políticas de control de acceso***
- ***Resumir rutas antes de publicarlas en el núcleo***
- ***Aislar el núcleo de las interrupciones o fallas de la capa de acceso***
- ***Enrutar entre las VLAN de la capa de acceso***

Los dispositivos de capa de distribución también se utilizan para administrar colas y priorizar el tráfico antes de realizar la transmisión a través del núcleo." (Cisco Systems, 2007)

5.1.14 ENLACES TRONCALES

"Los enlaces troncales a menudo se configuran entre los dispositivos de la red de la capa de distribución y de acceso. También se utilizan para transportar tráfico que pertenece a múltiples VLAN entre dispositivos mediante el mismo enlace. Al diseñar los enlaces troncales, debe considerarse los patrones de tráfico de la red y la estrategia VLAN generales." (Cisco Systems, 2007)

5.1.15 ENLACES DE CONTINGENCIA

"Cuando existen enlaces redundantes ente los dispositivos de la capa de distribución, estos dispositivos pueden configurarse para balancear la carga del tráfico a través de los enlaces. El balanceo de carga aumenta el ancho de banda disponible para las aplicaciones." (Cisco Systems, 2007)

5.1.16 IMPLEMENTACIÓN DE BLOQUES DE SWITCHES

"Los routers o switches multicapa generalmente se implementan en pares, con switches de capa de acceso divididos de manera equitativa entre los mismos. Esta configuración se denomina bloque de switch de departamento o construcción. Cada bloque de switches funciona de forma independiente, como resultado,

la falla de un único dispositivo no desactiva la red. Incluso la falla de todo un bloque de switches no afecta a un número considerable de usuarios finales." (Cisco Systems, 2007)

5.1.17 REDUNDANCIA EN LA CAPA DE DISTRIBUCIÓN

Los dispositivos en la capa de distribución tienen conexiones redundantes con los switches en la capa de acceso, estas conexiones proporcionan rutas alternativas. Al utilizar protocolo de enrutamiento adecuado en la capa de distribución, los equipos de capa 3 reaccionan rápidamente ante las fallas en los enlaces; por lo tanto, no afecta el funcionamiento de la red. (Cisco Systems, 2007)

"La utilización de varias conexiones con los switches de capa 2 puede provocar un comportamiento inestable en una red a menos se active el STP (protocolo de árbol de expansión). Sin el STP, los enlaces redundantes en una red de capa 2 pueden causar tormentas de broadcast. Los switches no son capaces de aprender de forma correcta los puertos; por lo tanto, el tráfico termina acumulándose en todo el switch. Al deshabilitar uno de los enlaces, el STP garantiza que solo esté activa una ruta entre dos dispositivos. Si falla uno de los enlaces, el switch vuelve a calcular la tipología de árbol de expansión y comienza a utilizar automáticamente el enlace alternativo." (Cisco Systems, 2007)

5.1.18 FILTRADO DEL TRÁFICO DE LA RED

"Para filtrar el tráfico de la red, el equipo examina cada paquete y luego lo envía o lo desecha, según las condiciones especificadas en la ACL. Existen 2 tipos de ACL para distintos propósitos. Las ACL estándar filtran el tráfico según la dirección de origen. Las ACL extendidas pueden filtrar según varios criterios, entre ellos:

- ***Dirección de origen***
- ***Dirección de destino***
- ***Protocolos***
- ***Números de puerto o aplicaciones***
- ***Si el paquete es parte de un flujo TCP establecido"*** (Cisco Systems, 2007)

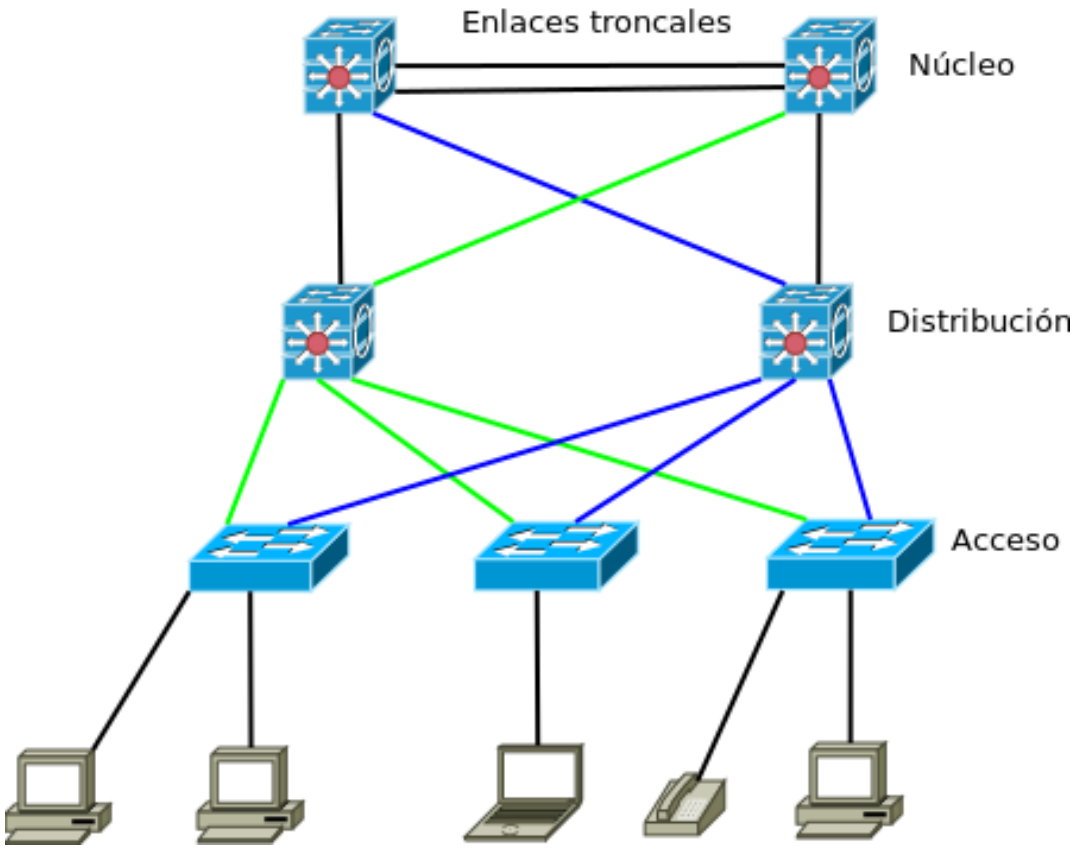


Fig. 2.- Capa de distribución
Fuente: Propia

5.2 ANALISIS DE LA SITUACIÓN ACTUAL DEL SISTEMA DE CABLEADO ESTRUCTURADO

El sistema de cableado estructurado del edificio del hospital en Portoviejo, fue implementado hace varios años cuando la norma de cableado aún permitía la instalación de sistemas de categoría 5E, debido al incremento de servicios y demanda de recursos este tipo de cableado está quedando obsoleto. Actualmente, no es la apropiada para el desarrollo de nuevas aplicaciones que requieren de altos anchos de banda. (Hernández, 2014)

El cableado inicial fue implementado sobre normas y estándares, lo que pudo apreciarse durante la inspección en sitio, pero con el paso del tiempo y en la medida que la red fue creciendo, no se mantuvieron los mismos, razón por la cual fue notorio observar cables que no tenían protección con ductos metálicos como es la recomendación de la norma y más aún por los niveles de seguridad que deben mantenerse dentro de un hospital.

A continuación, se detallan los aspectos de relevancia de un sistema de cableado, donde no se están cumpliendo las normas correspondientes.

5.2.1 CUARTO DE EQUIPOS

En esta área encontramos que los tubos de drenaje para el sistema de aguas servidas y la canalización de agua potable pasan sobre los racks, lo cual es inconsistente con las normas y estándares TIA 942, TIA 568-B.1. En caso de una rotura de tubería, el agua puede ocasionar daños irreversibles sobre los servidores que se encuentran en esta ubicación, así como los dispositivos activos. Es un punto muy crítico que debe ser corregido en el menor tiempo posible de preferencia con la implementación con un nuevo centro de datos que cumpla con las normas internacionales en cuanto a alta disponibilidad y seguridad. A demás, no se cuenta con un piso falso, ni un sistema adecuado de acceso.

Fig. 3.- Ductos sobre área de servidores
Fuente: Propia

Como recomendación se sugiere el cambio del recorrido de la canalización de agua servida y potable, o de otra forma migrar todos los equipos a un área libre de posibles canalizaciones de aguas; en el caso del cambio de área se debe cumplir con lo especificado en los estándares de la industria anteriormente mencionado [4][6]. Para ello se recomienda que:

- El cuarto de datos este provisto de un sistema de aterrizaje de unión equipotencial para correcto drenaje de corrientes parasitas y transientes de sobrevoltaje [4].
- El cuarto de equipos debería contar con piso falso para utilizar esta plataforma como turas de acceso y espacios de todos los sistemas que convergen al centro de datos, si el piso falso no aplica para esta infraestructura al menos debe instalarse un piso de vinil antiestático [4].
- El cuarto de equipos debería tener un sistema de control y acceso, este tendrá como dispositivo de autenticación lector de huellas [7].
- El cuarto de quipos tendría que ser provisto de un sistema de respaldo dedicado exclusivamente al área de datos y contar con un sistema de cableado estructurado inter rack entre el rack de telecomunicaciones y el rack de servidores [4][5]
- El cuarto de equipos debería constar con un sistema de detección y control de incendio. [8]

5.2.2 CUARTO DE TELECOMUNICACIONES

En esta área encontramos que la distribución del piso o conexión horizontal, están desconcentradas totalmente, tanto es así que existen en el cableado horizontal del hospital hasta 12 cuartos de telecomunicaciones, lo cual constituye un serio problema de administración, tomando en cuenta que en el momento que se presente un problema de conectividad, la revisión de la parte física tendrá más de un posible punto de quiebre, lo que hace mucho más difícil la detección y reparación del problema.

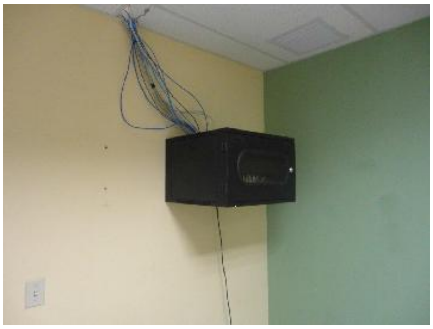


Fig. 4.- Rack aéreo 9
Fuente: Propia

Fig. 5.- Rack aéreo 2
Fuente: Propia

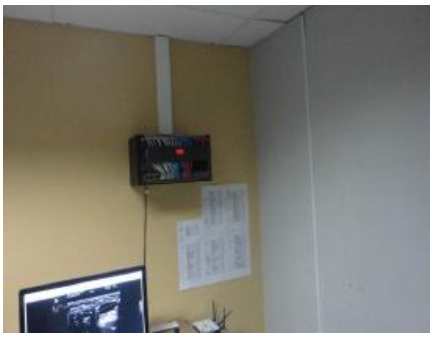


Fig. 6.- Rack aéreo 8
Fuente: Propia

Fig. 7.- Rack 3
Fuente: Propia

Fig. 8.- Rack 12
Fuente: Propia

Basándonos en la norma internacional TIA/EIA 568 un mínimo de un Cross-connect horizontal (HC) deberá ser provisto por cada piso y deberá haber un mínimo de un (HC) por cada 1,000 m2 de espacio reservado para las oficinas. Si el área del piso se extiende más allá de 1,000 m2 se deberá instalar (HC) adicionales para servir más eficientemente al área de trabajo.

Si un piso es escasamente poblado, es permisible servir este piso desde los Coss-connects horizontales localizados en un piso adyacente. La recomendación para esta área es instalar un máximo de 4 racks en planta baja uno master y 3 como adyacentes.

5.2.3 ENLACES ENTRE CUARTO DE TELECOMUNICACIONES MASTER MC Y CUARTOS DE TELECOMUNICACIONES ADYACENTES TR Y BACKBONE

En esta área los enlaces no se cumplen con la topología recomendada por las normas internacionales de la industria TIA/EIA 568.B3, 758.A. Los enlaces en la actualidad están instalados en serie, es decir, que existen varias interconexiones comprometiendo todo el sistema de backbone en un solo punto de falla.

La recomendación es la instalación de los enlaces en una topología jerárquica redundante según lo expuesto en las normas y estándares EIA/TIA 569 de buenos procedimientos de la construcción de backbone verticales, los enlaces deben estar bien identificados según el nivel al que correspondan.

Se deben construir los enlaces desde el MC hacia los diferentes TRs ubicados en los demás pisos y establecer el enlace redundante utilizando un cuarto de intermedio IC. Los enlaces deben utilizar un canal de transmisión de última generación con propiedades ópticas y mecánicas que permitan un ancho de banda de hasta 10Gbps, y una estructura ajustada que permita un correcto radio de giro en instalaciones interiores.

Fig. 9.- Conexiones Backbone
Fuente: Propia

5.2.4 CABLEADO HORIZONTAL - CANALIZACIÓN

La canalización existente es parcial ya que se encuentra instalado un electrocanal 10x10 sin tapa en todos los pisos y ductos para la distribución de los cable UTP, adicionalmente las ramales y bajantes están canalizadas en algunos casos con tubos empotrados y en otros con canaletas plásticas decorativas, así también en el crecimiento por movimientos adicionales y cambios existentes sobre una gran cantidad de cables que no cuentan con canalización y viajan libremente por encima del cielo falso.

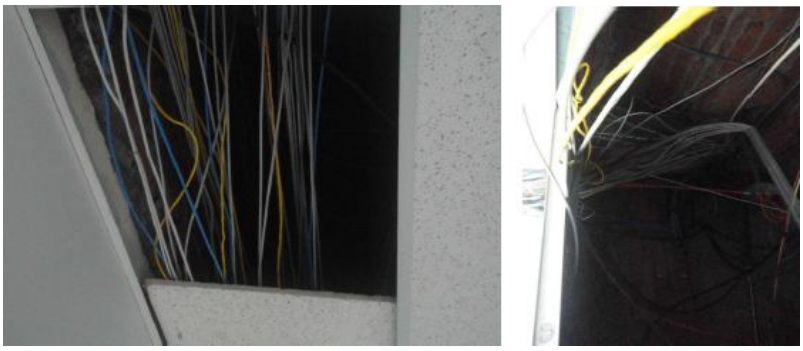


Fig. 10.- Estado del sistema del cableado horizontal
Fuente: Propia

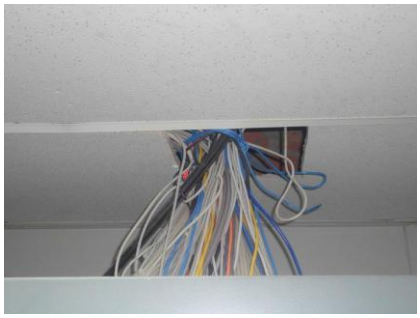


Fig. 11.- Estado del sistema del cableado vertical
Fuente: Propia

La recomendación para el sistema de canalización es utilizar TIA/EIA 569, instalar electrocanales 20x10 tipo bandeja ranura, tubos ¾ EMT y canalización perimetral para los ramales con canaletas decorativas sobrepuestas, para la bajante a los racks se debe utilizar bandejas de cables flexibles de 10x5 y 20x10 con accesorios que permitan el alojamiento de los cables y cuiden un grado de curvatura de 45 grados.

5.2.5 CABLE UTP

El cable categoría 5E, cuenta con un ancho de banda análogo de 100 MHz y un ancho de banda digital de 100 Mbps lo cual es suficiente para alojar plataformas y sistema como datos, VoIP, internet, bases de datos, sistemas de gestión, entre otros [9].

Pero como recomendación se debe instalar un tipo de cable UTP categoría 6A el mismo que cuenta con un ancho de banda análogo de 500Mhz y un ancho de banda digital de 10 Gbps [10].

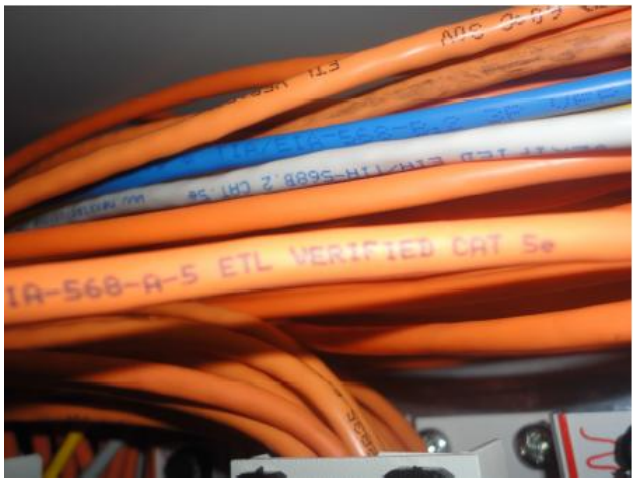


Fig. 12.- Cableado UTP categoría 5E
Fuente: Propia

5.2.6 ANÁLISIS DE LOS ELEMENTOS ACTIVOS DE RED (SWITCHS)

Uno de los aspectos que conlleva al presente estudio, es el bajo rendimiento de la red, lo cual en términos normales está determinado por aspectos como ancho de banda, retardos, fluctuaciones de retardos y paquetes perdidos [11].

En los actuales momentos la institución tiene aplicativos y servicios de misión crítica, como la transmisión de imágenes de alta resolución que requiere de un adecuado nivel de servicio, el mismo que debe estar determinado por la capacidad de los elementos de conmutación.

En la sección anterior se indicó que el sistema de cableado UTP categoría 5E no brinda el ancho de banda adecuado desde el punto de vista físico. Ahora nos encargaremos de analizar la parte lógica, el manejo de la capacidad de conmutación de los switches encontrados e instalados en la red.

El principal problema encontrado es que no se cuenta con una plataforma de equipos en común, pues existen una mezcla de switches administrables y no administrables, puertos de 10, 100 para estaciones de trabajo y 1000 Mbps para conexión al backbone, no hay estándares implementados en lo que a conmutación se refriere, pues lo equipos apenas soportan ciertas características técnicas recomendadas.

Se ha encontrado elementos de diferentes fabricantes como 3Com, Alcatel, D-Link, TP-Link. Salvo el primer fabricante mencionado, implementa características administrables en ciertos switches, los demás no. Esto

implica que, si se desea segmentar la red en VLANs, no es posible, pues la mayoría de switches de la red no lo soportan.

Lo mismo ocurre con la aplicación de Spanning Tree entre otros, no hay uniformidad en la plataforma de conmutación. En otros términos, todo se reduce a lo que el peor equipo pueda soportar, lo cual limita el rendimiento de la red.

Fig. 13.- Dispositivo de conmutación 3com
Fuente: Propia

Fig. 14.- Dispositivo de conmutación D-Link
Fuente: Propia

Los aplicativos modernos requieren de alta disponibilidad, soporte de IPv6, tráfico multicasting, soporte a calidad de servicio, seguridad a nivel de capa 2, entre otros [12].

La plataforma de conmutación actualmente implementada, no permite cumplir los aspectos mencionados.

No existe un conmutador de capa 3, la conmutación entre segmentos lógicos se lo hace por medio de un ruteador, lo que disminuye de forma crítica el rendimiento de la red.

El diseño de conmutación no existe, pues toda la red es plana. No se evidencia la implementación de un modelo jerárquico o en capas.

Se realizan conexiones en cascada entre otros elementos de capa 2, y al haber múltiples armarios con varios switches, esto trae consigo un incremento de latencia. El tráfico de extremo a extremo pasa por múltiples switches intermedios, cada uno de los cuales agrega latencia al tráfico de paquetes de red; más si a esto agregamos que elementos como DLink y TP-Link son completamente Store-Forward, he aquí la evidencia de bajo rendimiento es crítica.

A demás, hay que mencionar que no hay dispositivos de redundancia, que permitan que los puntos críticos de falla se comporten como FailOver, los elementos de cableado no son redundantes y no proveen rutas alternas ante fallas, tampoco los switches implementados evidencian aspectos de alta disponibilidad.

A continuación, se detallan los elementos de conmutación encontrados en la red (Tabla 1) y acorde a la capacidad de la planta de cableado existente (Tabla 2):

FABRICANTE	MODELO	UBICACION	PUERTOS
3Com	4500 x 2 3CR17562-91	Gabinete Principal	48 Puertos 10/100 Mbps 4 Uplinks de 1 Gbps
3Com	4200 3C17302A	Rack 3	48 Puertos 10/100 Mbps 2 Uplinks de 1 Gbps
3Com	4200 3C17302A	Rack 3	24 Puertos 10/100 Mbps 2 Uplinks de 1 Gbps
3Com	Super Stack 3 3C17304A	Rack 1	24 Puertos 10/100 Mbps 2 GBIC 1 Gbps UTP 2 GBIC 1 Gbps FO
3Com	4200 3C17302A	Rack 1a	48 Puertos 10/100 Mbps 2 Puertos Gbps UTP
Alcatel	Omnistack 6148	Rack 11	48 Puertos 10/100 Mbps
Alcatel	Omnistack 6148	Rack 12	48 Puertos 10/100 Mbps
D-Link	DES-3026 x 2	Rack computo	24 Puertos 10/100 Mbps 2 Uplinks de 100 Mbps
D-Link	DES-3526 x 1	Rack Servidores	24 Puertos 10/100 Mbps 2 Uplinks de 1 Gbps
D-Link	DES-3226S x 2	Rack 5	24 Puertos 10/100 Mbps 2 Uplinks de 100 Mbps
D-Link	DES-3226S x 2	Rack 6	24 Puertos 10/100 Mbps 10 Uplinks de 100 Mbps
D-Link	DES-3026	Rack 8	24 Puertos 10/100 Mbps 2 Uplinks de 100 Mbps
D-Link	DES-1024 x 2	Rack 10	24 Puertos 10/100 Mbps 2 Uplinks de 100 Mbps
TP-Link	TL-SG2224	Rack 9	24 Puertos 10/100 Mbps 2 Puertos GBIC x 1 Gbps

Tabla 1.- Puertos de los Switches

Fuente: Propia

IDENTEIFICACION	AREA	PUNTOS DE DATOS	PUNTOS DE VOZ
Rack 1	Gastroenterología	54	48
Rack 2	Informática	96	156
Rack 3	Jurídico	72	72
Rack 4	Guardianía	48	
Rack 5	Primer Piso HSP	48	48
Rack 6	Segundo Piso HSP	48	24
Rack 7	Informática	48	
Rack 8	Imagenología	24	
Rack 9	Laboratorio Clínico	19	
Rack 10	Informática		60
Rack 11	Mantenimiento	24	
Rack 12	Radioterapia	48	24

Tabla 2.- Puntos de voz y datos
Fuente: Propia

Como puede observarse no todos los switches pueden adaptarse al establecimiento de protocolos que puedan soportarse a lo largo de toda la infraestructura. Un ejemplo si se requiere implementar VLANs, no todos los equipos lo soportan, y aunque cubren la norma IEEE 802.1Q, existen diferencias entre fabricantes, lo que va en contra a la estandarización.

Otros puntos notables van por el lado del rendimiento, donde los switches 3Com ofrecen un buen rendimiento, pero el mismo baja a otro extremo con el uso de equipos como D-Link y TP-Link.

Todos soportan una capacidad acorde con el cableado existente, pero no con los requerimientos actuales de una red convergente de alto rendimiento; 10/100 Mbps ya no es una norma para áreas de trabajo y sobre todo para aplicativos como procesamiento de imágenes de alta resolución.

Ninguno de los Switches soporta IPv6, el nuevo estándar de direccionamiento IP establecido por la sociedad de internet.

Se implementa una manera no estándar de aspectos de calidad de servicio, no se tiene soporte a implementación de multicasting a excepción de los equipos 3Com de la serie 4500.

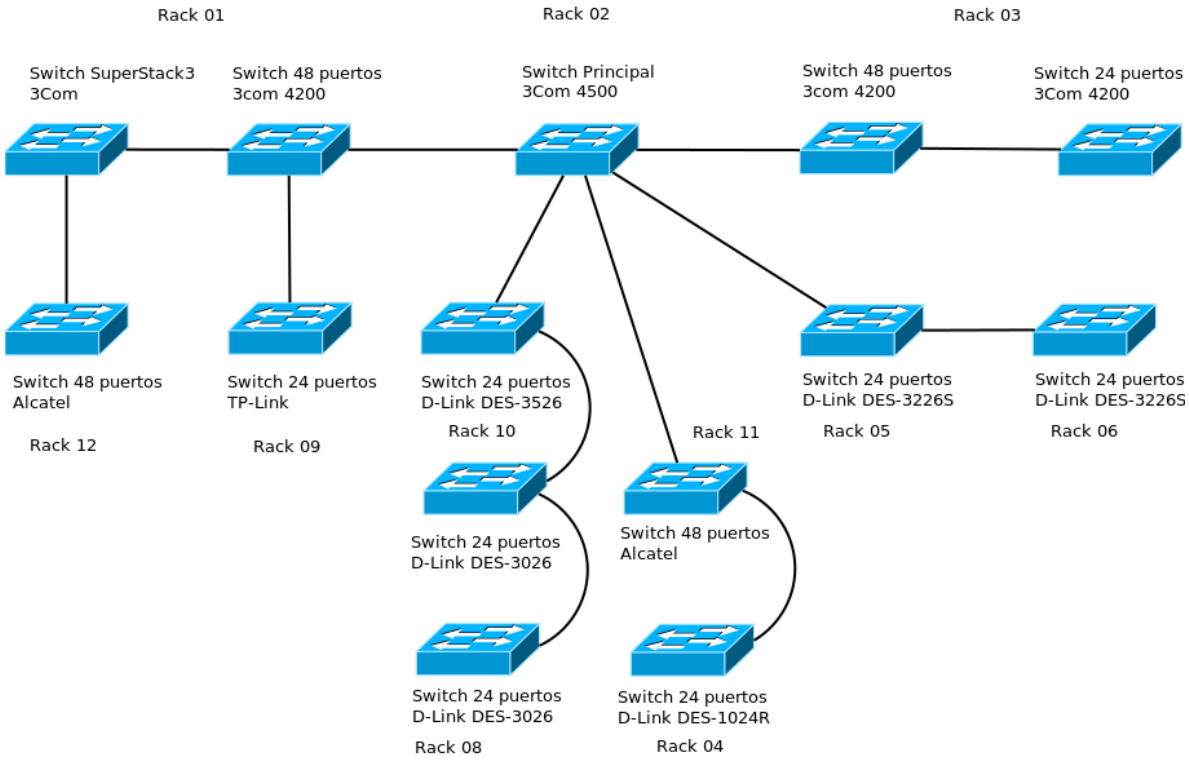


Fig. 15.- Diagrama de red del backbone principal actual

Fuente: Propia

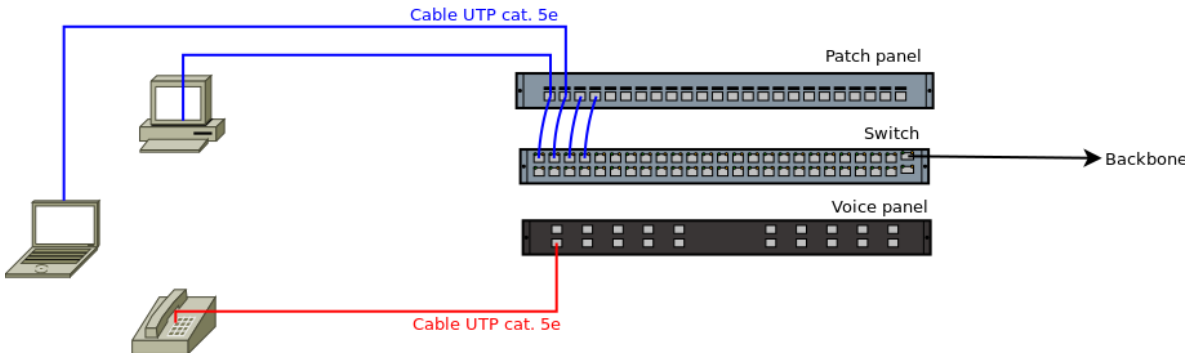


Fig. 16.- Diagrama de red del cableado horizontal

Fuente: Propia

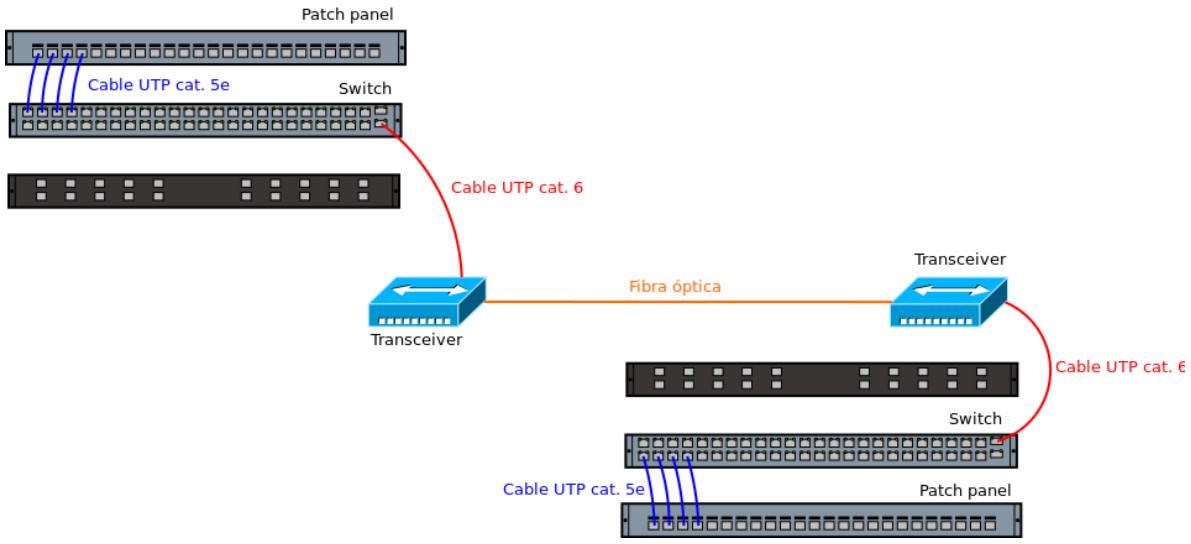


Fig. 17.- Diagrama de red del cableado vertical

Fuente: Propia

5.3 ANÁLISIS DE TRÁFICO DE LA RED

5.3.1 TRÁFICO DE LA RED Y PROTOCOLOS

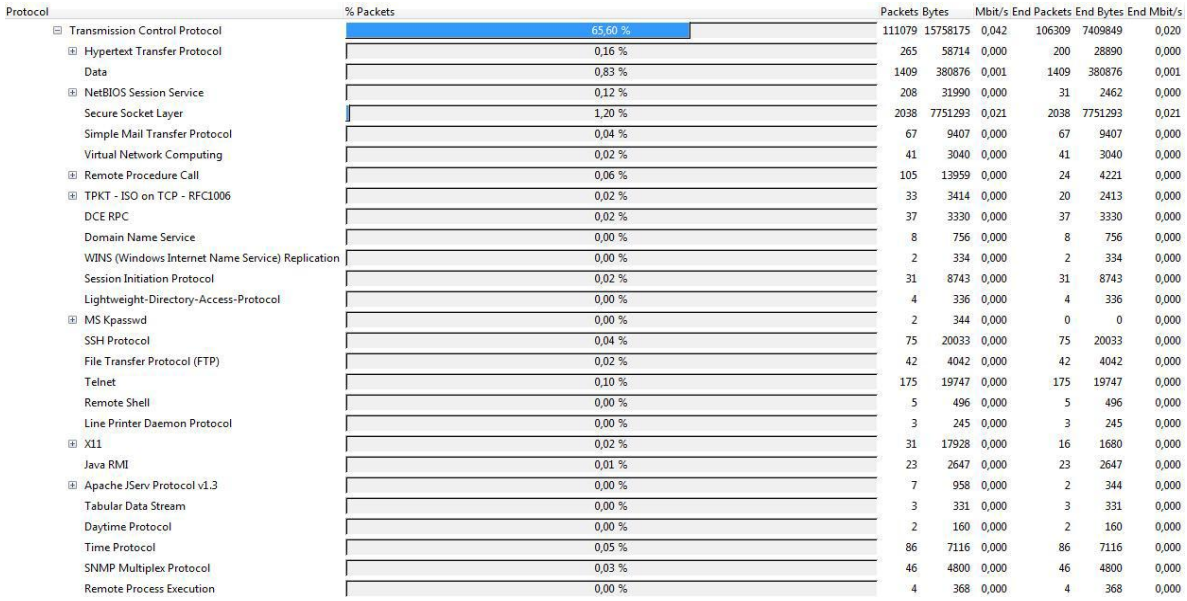
Se procede en hacer un análisis de tráfico en la red, utilizando para ello un software wireshark, un poderoso sniffer que permite una interfaz sencilla desglosando los paquetes capturados para comprender la estructura de los protocolos en lo que comprende al monitoreo, con el fin de establecer tendencias en cuanto al tipo de tráfico por protocolo. A continuación se describen algunas observaciones resultado de un estudio analizado respecto al tráfico:

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	169316	22702410	0,060	0	0	0,000
Ethernet	100,00 %	169316	22702410	0,060	0	0	0,000
Internet Protocol	92,71 %	156965	21458729	0,057	0	0	0,000
User Datagram Protocol	26,68 %	45181	5572818	0,015	0	0	0,000
Transmission Control Protocol	65,60 %	111079	15758175	0,042	106309	7409849	0,020
Internet Control Message Protocol	0,42 %	705	127736	0,000	705	127736	0,000
Logical-Link Control	1,26 %	2137	187825	0,001	0	0	0,000
Address Resolution Protocol	3,73 %	6309	364468	0,001	6309	364468	0,001
Internet Protocol Version 6	2,31 %	3904	691328	0,002	0	0	0,000
User Datagram Protocol	2,22 %	3760	678944	0,002	0	0	0,000
Internet Control Message Protocol v6	0,09 %	144	12384	0,000	144	12384	0,000
MDS Header	0,00 %	1	60	0,000	0	0	0,000

Fig. 18.- Tráfico general por protocolos
Fuente: Propia

Puede observarse que todo el tráfico en capa 2 es Ethernet y que lo que debe ser esperado es que la mayor parte del flujo sea IPv4. Sin embargo puede notarse que existe flujo IPv6 activo a pesar de no contar con un stack IPv6, lo cual da la idea que existen equipos o estaciones de trabajo con sistema Windows que trae activado por defecto el protocolo IPv6; lo que se sugiere es desactivar dicho protocolo ya que el mismo hace uso de peticiones multicast, como no es controlado por los switches presentes, finalmente se comporta como broadcast, el cual afecta el rendimiento y agrega latencia.

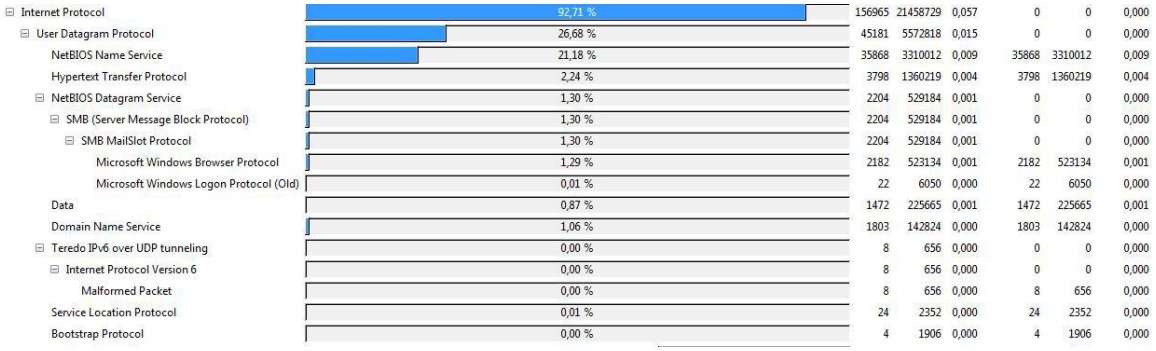
Lo siguiente es medir el flujo IPv4 de acuerdo a los protocolos de transporte TCP y UDP, obteniendo los siguientes datos:



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Transmission Control Protocol	65,60 %	111079	15758175	0,042	106309	7409849	0,020
Hypertext Transfer Protocol	0,16 %	265	58714	0,000	200	28890	0,000
Data	0,83 %	1409	380876	0,001	1409	380876	0,001
NetBIOS Session Service	0,12 %	208	31990	0,000	31	2462	0,000
Secure Socket Layer	1,20 %	2038	7751293	0,021	2038	7751293	0,021
Simple Mail Transfer Protocol	0,04 %	67	9407	0,000	67	9407	0,000
Virtual Network Computing	0,02 %	41	3040	0,000	41	3040	0,000
Remote Procedure Call	0,06 %	105	13959	0,000	24	4221	0,000
TPKT - ISO on TCP - RFC1006	0,02 %	33	3414	0,000	20	2413	0,000
DCE RPC	0,02 %	37	3330	0,000	37	3330	0,000
Domain Name Service	0,00 %	8	756	0,000	8	756	0,000
WINS (Windows Internet Name Service) Replication	0,00 %	2	334	0,000	2	334	0,000
Session Initiation Protocol	0,02 %	31	8743	0,000	31	8743	0,000
Lightweight-Directory-Access-Protocol	0,00 %	4	336	0,000	4	336	0,000
MS Kpasswd	0,00 %	2	344	0,000	0	0	0,000
SSH Protocol	0,04 %	75	20033	0,000	75	20033	0,000
File Transfer Protocol (FTP)	0,02 %	42	4042	0,000	42	4042	0,000
Telnet	0,10 %	175	19747	0,000	175	19747	0,000
Remote Shell	0,00 %	5	496	0,000	5	496	0,000
Line Printer Daemon Protocol	0,00 %	3	245	0,000	3	245	0,000
X11	0,02 %	31	17928	0,000	16	1680	0,000
Java RMI	0,01 %	23	2647	0,000	23	2647	0,000
Apache JServ Protocol v1.3	0,00 %	7	958	0,000	2	344	0,000
Tabular Data Stream	0,00 %	3	331	0,000	3	331	0,000
Daytime Protocol	0,00 %	2	160	0,000	2	160	0,000
Time Protocol	0,05 %	86	7116	0,000	86	7116	0,000
SNMP Multiplex Protocol	0,03 %	46	4800	0,000	46	4800	0,000
Remote Process Execution	0,00 %	4	368	0,000	4	368	0,000

Fig. 19.- Tráfico TCP

Fuente: Propia

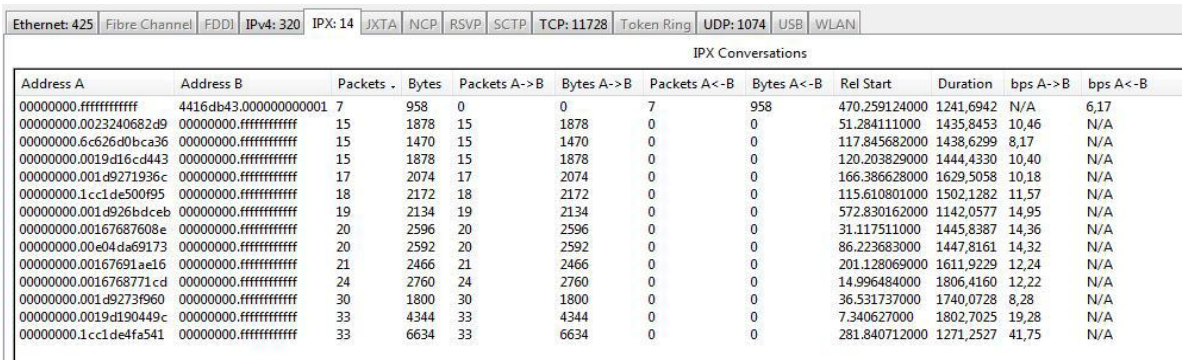


Internet Protocol	92,71 %	156965	21458729	0,057	0	0	0,000
User Datagram Protocol	26,68 %	45181	5572818	0,015	0	0	0,000
NetBIOS Name Service	21,18 %	35868	3310012	0,009	35868	3310012	0,009
Hypertext Transfer Protocol	2,24 %	3798	1360219	0,004	3798	1360219	0,004
NetBIOS Datagram Service	1,30 %	2204	529184	0,001	0	0	0,000
SMB (Server Message Block Protocol)	1,30 %	2204	529184	0,001	0	0	0,000
SMB MailSlot Protocol	1,30 %	2204	529184	0,001	0	0	0,000
Microsoft Windows Browser Protocol	1,29 %	2182	523134	0,001	2182	523134	0,001
Microsoft Windows Logon Protocol (Old)	0,01 %	22	6050	0,000	22	6050	0,000
Data	0,87 %	1472	225665	0,001	1472	225665	0,001
Domain Name Service	1,06 %	1803	142824	0,000	1803	142824	0,000
Teredo IPv6 over UDP tunneling	0,00 %	8	656	0,000	0	0	0,000
Internet Protocol Version 6	0,00 %	8	656	0,000	0	0	0,000
Malformed Packet	0,00 %	8	656	0,000	8	656	0,000
Service Location Protocol	0,01 %	24	2352	0,000	24	2352	0,000
Bootstrap Protocol	0,00 %	4	1906	0,000	4	1906	0,000

Fig. 20.- Tráfico UDP

Fuente: Propia

Al igual que el flujo IPv6 no habilitado, también se detectó tráfico de protocolo IPX, lo cual es extraño debido a constituir un protocolo obsoleto.



Ethernet: 425 | Fibre Channel | FDDI | IPv4: 320 | IPX: 14 | JXTA | NCP | RSVP | SCTP | TCP: 11728 | Token Ring | UDP: 1074 | USB | WLAN

IPX Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
00000000.ffffffffffff	4416db43.000000000001	7	958	0	0	7	958	470.259124000	1241,6942	N/A	6,17
00000000.0023240682d9	00000000.ffffffffffff	15	1878	15	1878	0	0	51.284111000	1435,8453	10,46	N/A
00000000.6c626d0bca36	00000000.ffffffffffff	15	1470	15	1470	0	0	117.845682000	1438,6299	8,17	N/A
00000000.0019d16cd443	00000000.ffffffffffff	15	1878	15	1878	0	0	120.203829000	1444,4330	10,40	N/A
00000000.001d9271936c	00000000.ffffffffffff	17	2074	17	2074	0	0	166.386628000	1629,5058	10,18	N/A
00000000.1cc1de500f95	00000000.ffffffffffff	18	2172	18	2172	0	0	115.610801000	1502,1282	11,57	N/A
00000000.001d926bdceb	00000000.ffffffffffff	19	2134	19	2134	0	0	572.830162000	1142,0577	14,95	N/A
00000000.00167687608e	00000000.ffffffffffff	20	2596	20	2596	0	0	31.117511000	1445,8387	14,36	N/A
00000000.00e04da69173	00000000.ffffffffffff	20	2592	20	2592	0	0	86.223683000	1447,8161	14,32	N/A
00000000.00167691ae16	00000000.ffffffffffff	21	2466	21	2466	0	0	201.128069000	1611,9229	12,24	N/A
00000000.0016768771cd	00000000.ffffffffffff	24	2760	24	2760	0	0	14.996484000	1806,4160	12,22	N/A
00000000.001d9273f960	00000000.ffffffffffff	30	1800	30	1800	0	0	36.531737000	1740,0728	8,28	N/A
00000000.0019d190449c	00000000.ffffffffffff	33	4344	33	4344	0	0	7.340627000	1802,7025	19,28	N/A
00000000.1cc1de4fa541	00000000.ffffffffffff	33	6634	33	6634	0	0	281.840712000	1271,2527	41,75	N/A

Fig. 21.- Tráfico IPX

Fuente: Propia

En este último la ventaja es que se muestran las direcciones MAC que tiene asignada cada equipo, esto es una evidencia clara de que hay tráfico no deseado que circula en la red de la institución y que debe ser eliminado para evitar comportamientos inadecuados.

La siguiente figura nos muestra otros comportamientos inadecuados, podemos observar un alto flujo multicast (239.255.255.250) del host 10.10.70.1. En caso de ser un tráfico autorizado, al no haber contención de broadcast en la red, el multicast toma este comportamiento, generando inconvenientes de inundación en la red. Cabe destacar que la saturación de la red viene considerándose como un tipo de ataque interno no premeditado ya que se da por incorrecta administración de la red.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B
192.168.0.0	192.168.0.15	4036	242372	2006	120360
192.168.101.23	192.168.101.31	1808	166336	1808	166336
192.168.0.188	192.168.0.255	1484	143494	1484	143494
10.10.70.1	239.255.255.250	1326	462366	1326	462366
192.168.0.6	192.168.0.15	2727	182671	1261	91614
192.168.0.1	192.168.0.15	2023	121656	1017	63328
192.168.0.8	192.168.0.15	2250	132414	1005	60300
192.168.0.2	192.168.0.15	2012	118658	1001	60060
192.168.0.9	192.168.0.15	2002	118108	1000	60000
192.168.102.40	192.168.102.47	852	78837	852	78837
192.168.102.34	192.168.102.47	789	73557	789	73557
192.168.102.121	192.168.102.127	781	72305	781	72305
192.168.101.69	192.168.101.71	697	64577	697	64577
192.168.0.15	192.188.59.30	1644	1539592	595	42231
192.168.102.60	239.255.255.250	426	167205	426	167205
192.168.0.188	224.0.0.252	342	23884	342	23884
192.168.0.10	192.168.0.15	4013	240491	328	23578
192.168.102.3	192.168.102.31	324	30261	324	30261
192.168.102.62	239.255.255.250	310	104724	310	104724
192.168.0.8	192.168.0.255	307	34177	307	34177
192.168.101.125	239.255.255.250	302	103842	302	103842
192.168.102.50	192.168.102.63	285	26673	285	26673
192.168.103.104	192.168.103.111	285	26673	285	26673
192.168.101.40	192.168.101.47	281	26637	281	26637
192.168.102.2	192.168.102.31	280	42340	280	42340
192.168.101.180	192.168.101.191	279	26121	279	26121
192.168.102.10	192.168.102.31	276	25845	276	25845
192.168.0.112	192.168.0.255	275	25602	275	25602
192.168.102.29	192.168.102.31	275	25602	275	25602
192.168.0.6	192.168.0.255	273	25569	273	25569

Fig. 22.- Tráfico multicast
Fuente: Propia

Por otro lado, se detectan varios bloques de IP en el mismo segmento físico. Los equipos no han sido configurados para segmentar la red en redes subredes, sin embargo se divide erradamente la parte lógica del direccionamiento IP, detectándose los siguientes bloques en la misma red física. Esto es ya una vulnerabilidad debido a que la segmentación no está protegida ante ataques ni mucho menos se evidencia la existencia de redes virtuales para una encapsulación de la información a nivel de acceso en capa 2 por puertos específicos.

Los segmentos de direccionamiento IP evidenciados son:

- 192.168.0.0
- 192.168.100.0
- 192.168.101.0
- 192.168.102.0
- 192.168.103.0

Esta configuración del servidor proxy crea un tráfico innecesario en la red, pues se está enviando un Gateway al flujo de cada segmento, pero luego regresa al mismo segmento físico consumiendo el recurso de ancho de banda. El tráfico de broadcast es alto y puede comprobarse en la figura 21 respecto a Ethernet.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B
HewlettP_cf:16:95	CompalIn_a1:87:96	4675	2173423	2641	1947458
Toa_00:40:d0	CompalIn_a1:87:96	4055	245848	2017	122076
HewlettP_16:bb:be	CompalIn_a1:87:96	4049	242471	354	25138
G-ProCom_09:3c:79	CompalIn_a1:87:96	2775	185155	1287	93174
CompalIn_a1:87:96	b4:99:ba:05:f3:ee	2256	132738	1247	72198
IntelCor_f1:fc:28	CompalIn_a1:87:96	2061	146152	32	2922
Pro-Nets_46:03:c6	CompalIn_a1:87:96	2014	118778	1003	60180
CompalIn_a1:87:96	d8:d3:85:b8:5e:14	2007	118372	1004	58192
CompalIn_a1:87:96	e0:69:95:c8:ae:ed	2001	116060	2000	116000
Intel_c1:93:5a	Broadcast	1830	164254	1830	164254
IntelCor_df:80:c8	Broadcast	1808	166336	1808	166336
00:27:19:1b:d2:aa	IPv4mcast_7f:ff:fa	1326	462366	1326	462366
3com_b5:a4:60	Spanning-tree-(for-bridges)_00	1066	68224	1066	68224
Wistron_5c:39:84	Broadcast	918	61385	918	61385
IntelCor_af:7f:ca	Broadcast	852	78837	852	78837
e0:69:95:c3:7d:d4	Broadcast	848	51268	848	51268
Intel_90:44:9c	Broadcast	840	78981	840	78981
e0:69:95:b3:83:c0	Broadcast	781	72305	781	72305
HewlettP_cf:16:95	Broadcast	749	58191	749	58191
Internet_b3:aa:d3	Broadcast	710	65357	710	65357
6c:62:6d:0b:c9:6d	Broadcast	469	32964	469	32964
IPv4mcast_7f:ff:fa	20:6a:8a:3b:b3:84	426	167205	0	0
G-ProCom_09:3c:79	Broadcast	356	30549	356	30549
Intel_c1:93:5a	IPv4mcast_00:00:fc	342	23884	342	23884
b4:99:ba:05:f3:ee	Broadcast	325	35257	325	35257
e8:39:35:4e:8b:6c	Broadcast	324	30261	324	30261
Xerox_b5:da:2d	IPv4mcast_7f:ff:fa	310	104724	310	104724
Xerox_b5:db:b6	IPv4mcast_7f:ff:fa	302	103842	302	103842
IntelCor_df:8a:8e	Broadcast	290	26973	290	26973
IntelCor_f2:0c:e5	Broadcast	289	26442	289	26442
e8:39:35:3c:c9:72	Broadcast	289	42880	289	42880
e8:39:35:5d:89:37	Broadcast	288	26853	288	26853
00:27:0e:05:52:44	Broadcast	284	26817	284	26817
e8:39:35:4b:96:c0	Broadcast	282	26301	282	26301
e8:39:35:4a:df:d8	Broadcast	276	25845	276	25845

Fig. 23.- Tráfico Broadcast
Fuente: Propia

El análisis también muestra errores en tramas Ethernet y de IPv6, las primeras se detecta que son tipo especial de paquete enviado por los switches ALCATEL, mientras que la segunda se produce al utilizarse una dirección multicast IPv6 que intenta comunicarse con todos los nodos de IPv6, generando inconsistencias, la siguiente

figura da una idea de lo indicado. Se tiene en cuenta que al existir exceso de multicast corre el riesgo de que la red colapse y se vea afectada la integridad de la LAN.

Errors: 29 Warnings: 279 Notes: 877 Chats: 100022 Severity filter: Errors only

No.	Sever.	Group	Protocol	Summary
1474	Error	Malformed	Ethernet	Length field value goes past the end of the payload
1531	Error	Malformed	Ethernet	Length field value goes past the end of the payload
7593	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
8009	Error	Malformed	Ethernet	Length field value goes past the end of the payload
8158	Error	Malformed	Ethernet	Length field value goes past the end of the payload
13769	Error	Malformed	Ethernet	Length field value goes past the end of the payload
14001	Error	Malformed	Ethernet	Length field value goes past the end of the payload
14070	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
21517	Error	Malformed	Ethernet	Length field value goes past the end of the payload
21772	Error	Malformed	Ethernet	Length field value goes past the end of the payload
23421	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
26364	Error	Malformed	Ethernet	Length field value goes past the end of the payload
26500	Error	Malformed	Ethernet	Length field value goes past the end of the payload
28908	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
31256	Error	Malformed	Ethernet	Length field value goes past the end of the payload
31514	Error	Malformed	Ethernet	Length field value goes past the end of the payload
31884	Error	Malformed	FC	Malformed Packet (Exception occurred)
55919	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
58423	Error	Malformed	Ethernet	Length field value goes past the end of the payload
58646	Error	Malformed	Ethernet	Length field value goes past the end of the payload
67623	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
68224	Error	Malformed	Ethernet	Length field value goes past the end of the payload
68706	Error	Malformed	Ethernet	Length field value goes past the end of the payload
139628	Error	Malformed	Ethernet	Length field value goes past the end of the payload
140240	Error	Malformed	Ethernet	Length field value goes past the end of the payload
141832	Error	Malformed	IPv6	Malformed Packet (Exception occurred)
163312	Error	Malformed	Ethernet	Length field value goes past the end of the payload
164072	Error	Malformed	Ethernet	Length field value goes past the end of the payload
168678	Error	Malformed	IPv6	Malformed Packet (Exception occurred)

Fig. 24.- Errores detectados
Fuente: Propia

En consideración al análisis realizado es notorio que como resultado se observa que dicha infraestructura lógica actualmente está expuesta a múltiples ataques que podrían darse, como por ejemplo la denegación de servicios DDoS, que causaría que la red se atenúe colapsando el recurso y consumiendo el total de ancho de banda disponible en general.

5.3.2 MITIGACIÓN

Se considera prioritario implementar un diseño que permita la segmentación lógica de manera efectiva y que al mismo tiempo sea de alto rendimiento, para ello se deberá sugerir un switch con capacidad de conmutar en capa 3.

"La utilización de VLAN y subredes IP es el mecanismo más común para segregar grupos de usuarios y tráfico de la red de la capa de acceso" (Cisco Systems, 2007), además de ello hace que la seguridad y el rendimiento sean mejores, debido a que si existiese un ataque a una determinada VLAN, las demás no se verán afectadas.

En la actualidad, las VLAN se utiliza para separar y clasificar flujos de tráfico, además de controlar el broadcast dentro de un único armario de cableado; si bien las redes virtuales grandes que abarcan redes enteras ya no son recomendables, estas pueden ser necesarias para admitir aplicaciones especiales, como servicios de roaming y teléfonos IP. El método recomendado es contener las redes virtuales dentro de un único armario de cableado, esta modalidad aumenta la cantidad de VLAN en una red, lo cual también incrementa el número de subredes IP individuales. La recomendación es asociar una única subred IP con una única VLAN. El direccionamiento IP en la capa de acceso pasa a ser un aspecto de diseño esencial que afecta la escalabilidad de toda la red. (Cisco Systems, 2007)

5.3.3 PROVISIÓN DE CALIDAD DE SERVICIO EN LAS APLICACIONES DE RED

Las redes deben prestar servicios seguros, medibles y garantizados, por lo que también necesitan mecanismos para controlar la congestión cuando aumenta el tráfico. La congestión se produce cuando la demanda de recursos de red supera la capacidad disponible. Todas las redes tienen recursos limitados, por tal razón, las redes necesitan de implementación de servicio de calidad de servicio, clasificando el tráfico a la prioridad designada. (Cisco Systems, 2007)

5.3.4 CLASIFICACIÓN DE TRAMAS

Antes de asignar estrategias de QoS, es necesario clasificar las aplicaciones según los requerimientos específicos de entrega. La clasificación de datos en el origen o cerca del mismo permite asignar a dichos datos la prioridad adecuada a medida que se trasladan a través de toda a la red. La segregación en clases de tráfico con características similares y luego la identificación de dicho trafico mediante marcas, es la función de los dispositivos de red en las capas de distribución y de acceso. Un ejemplo de esta estrategia es colocar tráfico de voz de un switch de acceso en una única VLAN, luego, el dispositivo marca el tráfico que se origina desde la VLAN de voz con la máxima prioridad.

5.3.5 PROVISIÓN DE SEGURIDAD FÍSICA

"La seguridad física de una red es muy importante, la mayoría de los intrusos de la red obtienen acceso físico en la capa de acceso. En algunos dispositivos de red, como los routers y switches, el acceso físico puede permitir cambiar contraseñas y obtener acceso total a los demás dispositivos. Las medidas evidentes, como cerrar con llave los armarios de cableado y restringir acceso a los dispositivos, a menudo son las formas más efectivas de prevenir rupturas de seguridad. En áreas de fácil acceso o de alto riesgo, quizás sea necesario equipar los armarios de cableado con seguridad adicional, como cámaras o alarmas y dispositivos de detección." (Cisco Systems, 2007)

5.3.6 SEGURIDAD DE LOS DISPOSITIVOS DE RED EN LA CAPA DE ACCESO

"Las siguientes medidas simples pueden proporcionar seguridad adicional a los elementos activos de red en la capa de acceso:

- ***Configuración de contraseñas seguras***
- ***Utilizar SSH para administrar dispositivos***
- ***Deshabilitar puertos sin usar***

La seguridad de puerto del switch y el control de acceso a la red pueden asegurar que solo los dispositivos confiables y conocidos tengan acceso a la red. Los riegos de seguridad no pueden eliminarse por completo;

una efectiva evaluación y administración de riesgos puede reducir de manera considerable los riegos existentes. Al considerar las medidas de seguridad, es importante entender ningún protocolo puede garantizar la seguridad de la información. La verdadera seguridad de la red surge de una combinación de productos, servicios y procedimientos, junto con una cuidadosa política de seguridad y el compromiso para adherirse a esa política." (Cisco Systems, 2007)

5.4 CONSIDERACIONES DE ALTO RENDIMIENTO Y DESCRIPCION DE LAS TOPOLIGIAS FISICAS Y LOGICAS DE LA RED

5.4.1 MODELO JERÁRQUICO DE CAPAS

De acuerdo al escenario de diseño planteado, se propone implementar una red jerárquica de dos capas: distribución y acceso.

Una de las características que en la actualidad es un problema es la falta de segmentación lógica real, lo cual se solucionaría con la implementación y soporte de redes virtuales (VLANs). Los dispositivos a sugerir deberán soportar protocolos como IEEE 802.1Q e ISL. Así mismo deberá soportar la implementación de protocolo de enlace troncal dinámico (DTP); además de igual forma una implementación extremo a extremo de VLANs deberá proveer de protocolo de enlace troncal en red virtual (VTP).

Para el caso de la capa de distribución se debe recomendar un dispositivo switch de capa 3, con un alto rendimiento superior a 30 millones de paquetes por segundos, este elemento al mismo tiempo actúa como núcleo de la red por lo que su capacidad debe ser muy alta para soportar el tráfico de los segmentos y redes virtuales que se implementen dentro de la institución, también para el soporte de futuras aplicaciones como comunicaciones unificadas como soporte de voz y video.

Debe garantizar conexiones hacia los elementos de capa de acceso al menos 1 Gbps, y soportar protocolos que permitan la agregación de canales o puertos, de tal manera que si un segmento requiere de 2 a 3 Gbps, se lo pueda asignar. Así mismo debe tener conexiones con otro elemento de distribución, al menos con puertos en el orden de 10 Gbps como capacidad agregada.

Deberá mantener redundancia, ya sea por medio físico como fuente de alimentación, ventilación o elementos de conmutación que actúen rápidamente en caso de fallos, garantizando la continuidad operativa en la red.

Eso también puede asociarse con el soporte de protocolos como Spanning Tree, y protocolos como HSRP, que ofrece redundancia del default Gateway.

El soporte de tráfico multicasting, lo que implica soporte de IGMP (Internet Group Management Protocol) y en lo posible de MVR (Multicast VLAN Registration). Así también debe soportar protocolos de administración como SNMP, RMON; permitir conexiones vía SSH, HTTP y HTTPS. En lo que respecta a protocolos de enrutamiento deberá soportar EIGRP y/o OSPF.

En este switch deberán concentrarse todas las conexiones verticales provenientes de los diferentes armarios contemplados en el proyecto de reestructuración de la red, ofreciendo para ello módulos y puertos SPF para fibra óptica multimodo de 50 micrones. Deberá ser escalable en la parte de puertos, de tal forma que permita crecimiento futuro de nuevas áreas de red y armarios de cableado, así como permitir la agregación de puertos que puedan ser utilizados para efectos de redundancia.

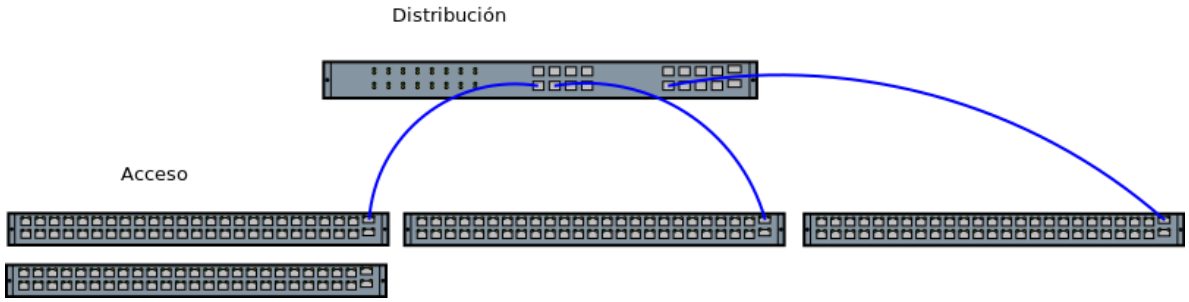


Fig. 25.- Modelo capa 2
Fuente: Propia

5.4.2 MECANISMO DE SEGURIDAD APLICADO A NIVEL DE CAPA 2 O ENLACE

Para lo que respecta al mecanismo de seguridad deberá soportar protocolos como MACSEC, autenticación basada en el estándar IEEE 802.1X, deberá permitir seguridad a nivel de puertos mediante el aprendizaje dinámico de las direcciones de capa 2 o direcciones físicas. Para un mejor rendimiento óptimo de los segmentos, el switch de distribución deberá soportar control de tormentas de broadcast y multicast.

Para una futura agregación de telefonía IP, tendrá que soportar VLAN VOICE; así mismo deberá proveer mecanismos de detección de errores en capa 2 como el uso de traceroute. También es importante que cumpla con el soporte de los siguientes protocolos:

- DHCP, para la asignación dinámica de direcciones y que la misma sea confiable gracias a la implementación de DAI (Dynamic ARP Inspection) y Snooping.
- IP SLAs, mecanismo que permite asignar factores de QoS a las aplicaciones críticas de cualquier institución.
- Auto QoS, mecanismo que permite detectar dispositivos para aplicar políticas de calidad de servicio por puerto.
- RSPAN, para análisis de tráfico o futura agregación de un IDS a la infraestructura de la red.
- NTP, para soportar la implementación de un registro de eventos de la red por medio de syslog.

Para proveer de los servicios y protocolos mencionados con anterioridad se recomienda un dispositivo switch de la familia 3750 de Cisco Systems.

5.4.3 INCORPORACION DE EQUIPOS FIREWALLS

Los servidores del centro de datos pueden ser blanco de ataques malintencionados y deben protegerse. Los ataques contra las granjas de servidores pueden originar perdidas económicas, para las aplicaciones interinstitucionales y de comercio en línea, además de generar robos de información. (Cisco Systems, 2007)

Deben protegerse tanto las redes de área local como las redes de área de almacenamiento (storage), para reducir las posibilidades de que ocurran dichos ataques. Los atacantes informáticos utilizan diferentes herramientas para inspeccionar las redes e iniciar ataques de intrusión y de denegación de servicio (DoS).

Durante la instalación de firewalls, estos no componen ninguna regla configurada, se deben establecer las políticas de seguridad que debe proporcionar a la red; básicamente debe constar de dos políticas generalizadas que son las de accesos permisivos y restrictivo. La política permisiva se trata de aceptar y dejar pasar todo trafico existente pero poco a poco ajustando las reglas de acceso. Por otra parte la política restrictiva es negar todo tráfico y poco a poco ir proporcionando acceso, al mismo tiempo proporcionando las reglas de seguridad.

La incorporación de equipos firewalls nos permitirá bloquear el paso de cierto tipo de información escuchando la totalidad del tráfico que circula, desarmar los encabezados de cada protocolo y estar en capacidad de decisión de filtrar información que tiene destino a un host especifico de la red, garantizando

que la información que fluya dentro de nuestra LAN se encuentre protegida ante intentos de ataques internos y externos.

Como otra medida de seguridad aplica la implementación de un IDS (sistema de detección de intrusos), el cual básicamente es un sniffer de red para seleccionar tráfico deseado notificando mediante alarmas alguna anomalía que se presente. La configuración más básica es agregarlo de tal forma que intercepte todo el tráfico en la red mediante 2 tarjetas de red, una para la red externa y la otra para el acceso a la LAN.

5.4.4 ZONAS DESMILITARIZADAS DMZ

"En el diseño tradicional de firewall de red, los servidores a los que se accedía desde las redes externas se ubicaban en la zona desmilitarizada. A los usuarios que accedían a estos servidores desde internet o desde otras redes externas poco confiables se les impedía ver los recursos ubicados en la LAN interna. Los usuarios de la LAN eran considerados usuarios confiables y generalmente tenían pocas restricciones cuando accedían a los servidores en una DMZ."

Para brindar una capa de seguridad adicional, generalmente es necesario que las granjas de servidores proporcionen una disponibilidad alta para los servicios y aplicaciones de red. Una red de alta disponibilidad es aquella que elimina o reduce el impacto potencial de fallas, esta protección permite que la red pueda cumplir con los requisitos de acceso a las aplicaciones y a los datos desde cualquier lugar. (Cisco Systems, 2007)

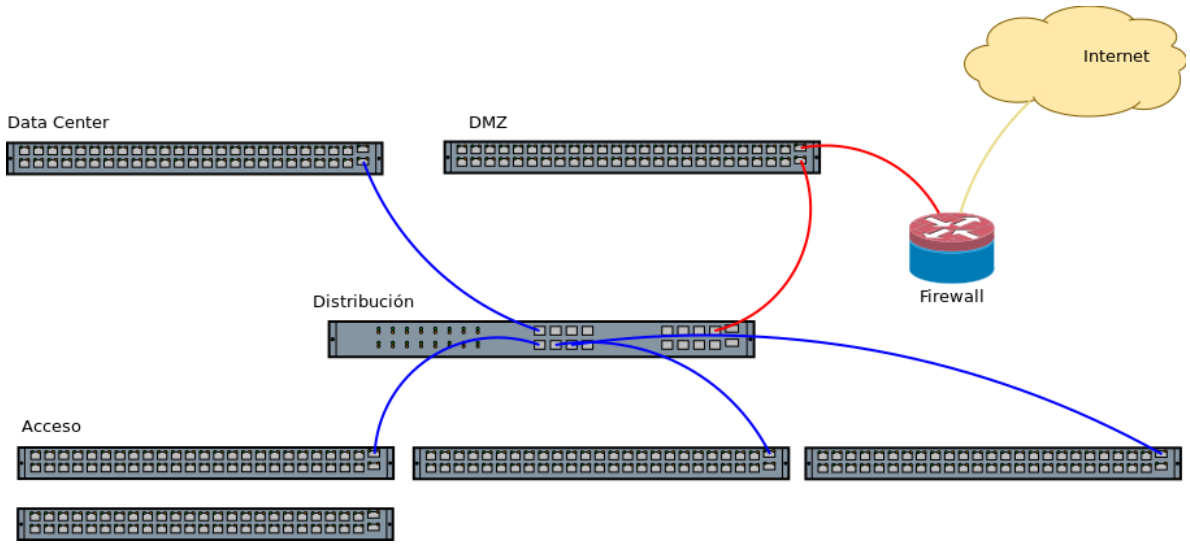


Fig. 26.- Mecanismo de seguridad
Fuente: Propia

5.4.5 TOPOLOGÍA FÍSICA

Para la implementación de la capa de acceso, con base a los requerimientos, se ha considerado switches de la serie 2960 de Cisco System. Debido a la densidad de puntos que se va a manejar en cada centro de cableado, estos dispositivos deben soportar Stack. Actualmente se manejan como stadalone, lo cual simplemente agrega latencia al tránsito de paquetes.

El mejor ejemplo es el rack de sistemas, donde convergen 145 puntos de datos. En lugar de manejar varios switches de 48 0 24 puertos, y todos ellos conectados en cascada, el stack permitirá que actúen como si fuesen uno solo, gracias a la conectividad del backplane de cada switch. Esto nos permitirá disponer de un súper switch de 144 0 192 puertos, en lugar de 3 o 4 de 48 puertos.

La diferencia en eficiencia sería notoria, pues se manejará una única tabla de puertos mac, las tramas pasaran por un único análisis de conmutación en capa de acceso. Las demás características son similares a las descritas en el switch de distribución, con la diferencia que los de capa de acceso no soportan capacidades de enrutamiento, ni funciones de implementación de políticas como las listas de acceso.

Los switches de capa de acceso considerados deben tener conexiones a los elementos de distribución, redundantes o no, al menos en el orden de 1 Gbps, mediante módulos de fibra óptica multimodo de 50

microns. Para el caso de que esta capacidad en algún momento futuro sea insuficiente, se cuenta con hasta 4 interfaces tipo Uplinks, de tal forma que mediante la implementación de PAgP o LACP, se pueda agregar canales hasta 2, 3, 4 Gbps o según lo requerido.

En caso de ser requerido en algún escenario, se puede agregar a estos switches la capacidad de soportar POE o potencia sobre Ethernet, lo que permitiría suministrar energía a estos elementos (usuario-final), como cámaras ip, teléfonos ip, puntos de acceso, u otros, cuyo consumo de recursos de energía sean soportados por la característica de POE.

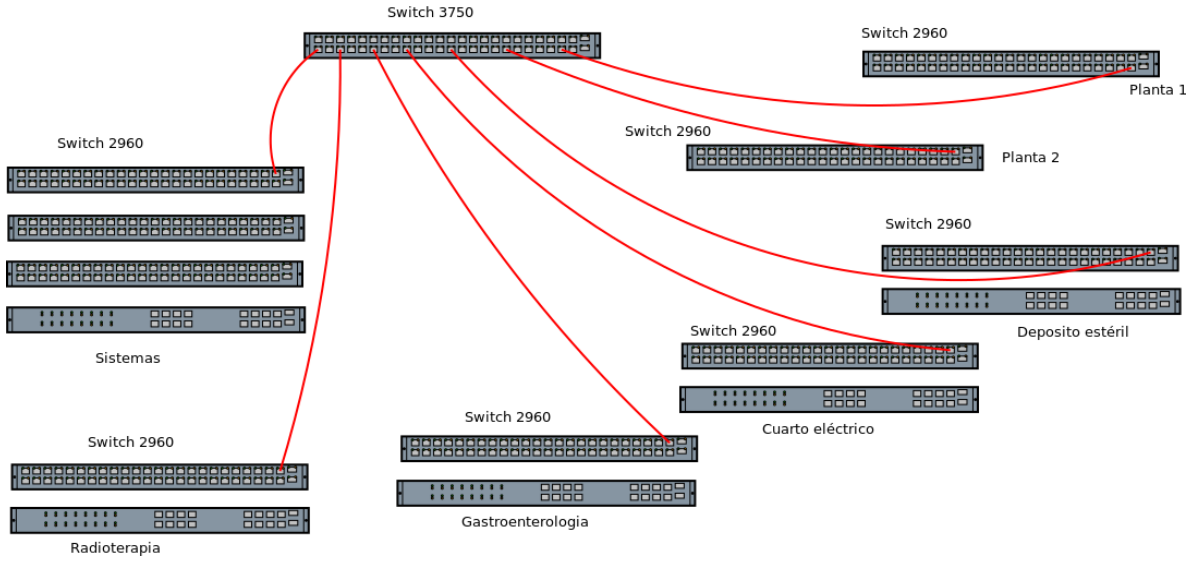


Fig. 27.- Topología física
Fuente: Propia

5.4.6 TOPOLOGÍA LÓGICA

La conectividad al centro de datos y servidores se la realizaría por medio de un enlace de fibra óptica para permitir alta capacidad de tráfico. Se utilizará para ello un switch de capa 2 con soporte de VLAN de tal manera que podemos implementar una VLAN llamada servidores, donde se accederá exclusivamente a los servidores internos o bases de datos de la institución.

Existirá otra VLAN denominada DMZ donde se alojaran los servidores tipo Enterprise y cuyos servicios sean semipúblicos, como correo electrónico, DNS server, o servidores WEB, esto a través de un firewall correctamente configurado para admisión de determinada de ciertos puertos; de esta forma no se compromete la seguridad de los servidores internos.

Para la mejora sustancial de acceso seguro a la información y red de comunicaciones de la institución se ha considerado un firewall tipo ASA con varias interfaces, que permitan la implementación de varias DMZ y conectividad de la red interna a la red externa como internet.

5.4.7 DESCRIPCIÓN DE ESCENARIO REDUNDANTE

Para aplicar una descripción de escenario redundante se parte de la distribución hacia los demás switches de la integración como lo sería en la figura siguiente.

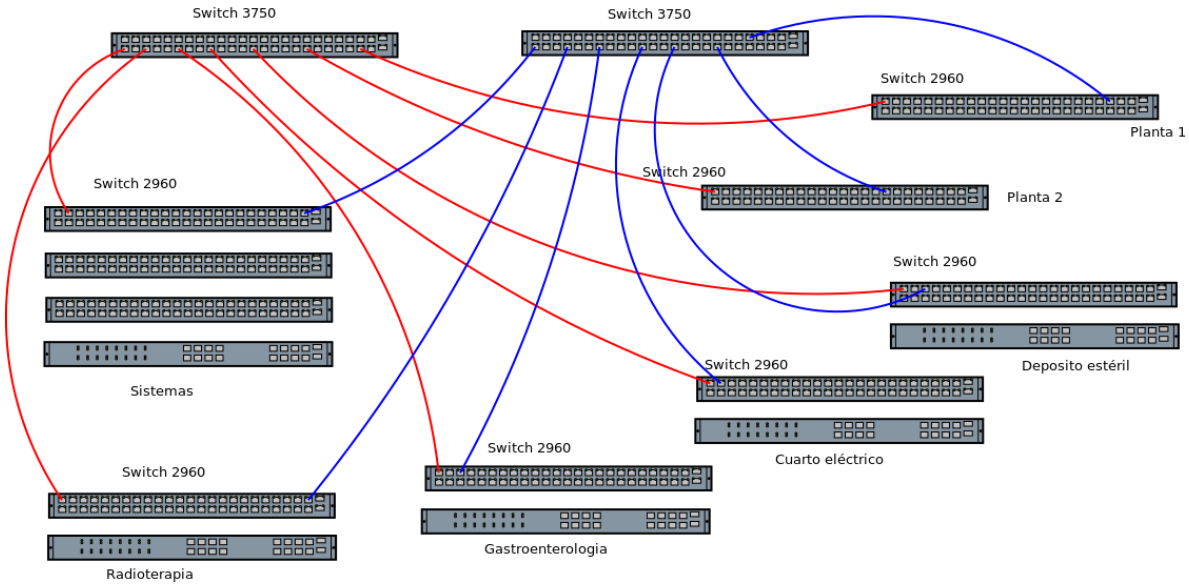


Fig. 28.- Escenario redundante

Fuente: Propia

5.4.8 WLAN

5.4.8.1 DISEÑO FISICO

En los diseños típicos de red inalámbrica, la mayor parte del esfuerzo se concentra en las áreas de cobertura física de la red. El diseño lleva a cabo un revelamiento del sitio a fin de determinar las áreas de cobertura de la red y encontrar ubicaciones óptimas para establecer puntos de acceso inalámbrico. Los resultados del revelamiento del sitio permiten determinar el hardware del punto de acceso, los tipos de antenas y los conjuntos de funciones inalámbricas deseadas. Se debe determinar si se puede admitir el servicio de roaming entre las áreas de cobertura superpuestas. (Cisco Systems, 2007)

5.4.8.2 DISEÑO LOGICO DE LA RED

La red compartida a menudo desea proporcionar diferentes niveles de acceso y distintos tipos de usuarios inalámbricos. Además, las redes inalámbricas deben ser seguras y fáciles de usar. La determinación de las funciones deseadas y las limitaciones implica diferentes maneras de diseñar y configurar las LAN inalámbricas.

Para asegurar el acceso del empleado, utilice una infraestructura WLAN completamente separada que no incluya el acceso para visitantes. Se recomienda separar los usuarios internos en una VLAN distinta. En otras áreas donde se restringe el acceso inalámbrico seguro en algunos dispositivos, se puede hacer uso de los filtros de direcciones MAC para limitar el acceso. (Cisco Systems, 2007)

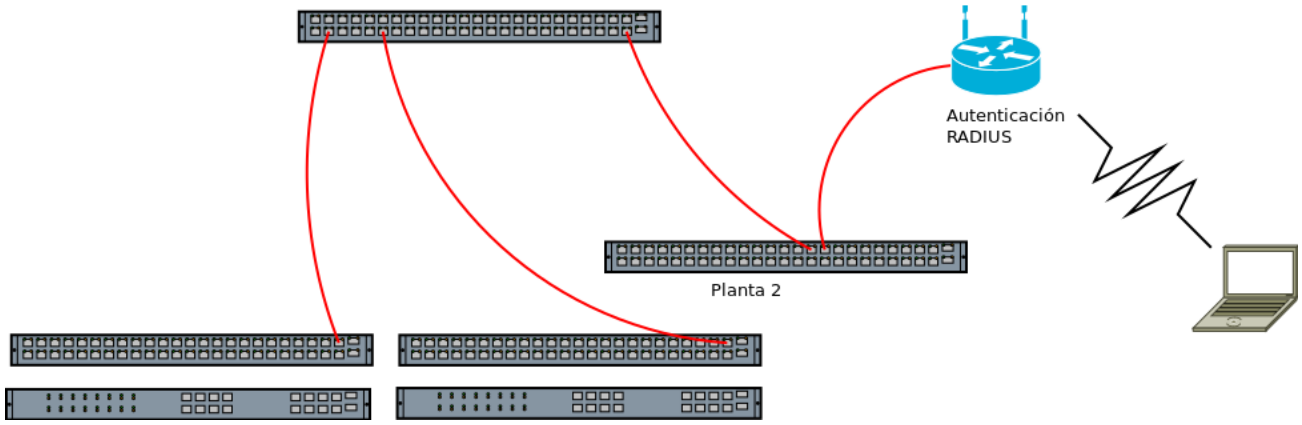


Fig. 29.- Autenticación RADIUS
Fuente: Propia

5.4.8.3 IMPLEMENTACION DE RADIUS PARA SERVICIO INALAMBRICO

Debido a la posibilidad de brindar accesibilidad a la red mediante dispositivos inalámbricos, es conveniente que se implemente mecanismos de seguridad, en el cual uno de ellos es la utilización del protocolo RADIUS que permite establecer conexiones específicamente en el puerto 1812 y 1813 para UDP, autenticando los accesos de dispositivos con un proceso de validación de usuario y contraseña. Dentro de una autenticación legítima se establecen políticas establecidas de seguridad determinando el tipo de usuario que accede a la red, se controlan previamente establecidas en configuración, la utilización de recursos necesarios.

Una de las características importantes de RADIUS es la capacidad de manejo de sesiones, el mismo que notifica el comienzo y finalización de conexiones y reportería de consumo de datos. Este protocolo se encuentra definido en la referencia RFC 2865 [1].

6 CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

En referencia al presente trabajo se puede determinar que existe diversidad de técnicas para el mejoramiento de una red de comunicación como lo es el presente caso. Se consideró una manera de asegurar la información adecuando una solución considerando los servicios que la institución brinda, evaluando la tecnología que ya está implementada y cuyas necesidades se han incrementado, lo cual se contempla y sugiere la adquisición de nuevos equipos con el fin de garantizar la seguridad de la información.

La utilización de equipos dentro de la infraestructura actual es útil únicamente con las bondades del cableado en categoría 5e, lo que determinaría únicamente que el recorrido queda para efectos de respaldo emergente, ya que se pretende el mejoramiento con de adaptación de nueva infraestructura con alcance a cableado 6A y la solución planteada en el presente estudio.

La modernización de los equipos activos va a ser clave en la implementación, mismos que vienen dotados con características acordes a los estándares y flexibles a tipos distintos de configuraciones lo que brindará una mejor garantía de resguardo de la información y soporte. Se incorporará una nueva línea a partir del nuevo esquema y será CISCO SYSTEM.

Los parámetros de configuración de los equipos activos de la red serían distintos a los que se utiliza en la actualidad, contemplando una correcta lógica de distribución permitiendo garantizar la seguridad que la información que circula en la red.

6.2 RECOMENDACIONES

Pese al mejoramiento planteado que garantice la información de la institución no está demás seguir ciertos lineamientos de precaución que aporte al resguardo y seguridad de los datos entre los cuales se mencionará a continuación:

- En virtud de la necesidad a los nuevos servicios de red para la institución se ha optado en proponer y adaptar una modelo de seguridad a nivel de capa 2 y protección con apoyo de corta fuegos para control de accesos internos así como desde el exterior, pero se deben ir mejorando a medidas a partir que vayan mejorando las tecnologías y modalidades de operar en la red.

- La utilización de materiales para el nuevo cableado debe cumplir estrictamente con las normas de fabricación legitimas acorde lo planteado.

- La adquisición de equipos debe cubrir las garantías técnicas del fabricante y mantener un acuerdo de soporte para casos específicos.

- Mantener una preservación de los equipos antiguos para efectos de respaldo emergente.

- En lo que concierte a la lógica de la red, la configuración deberá en lo posible mantener siempre la escalabilidad en los patrones de configuración.

- Para un mejor rendimiento y desempeño de la red, se recomienda que cada equipo activo no administre más de tres configuraciones de VLANS distintas o de ser el caso por necesidad se deberá reforzar el equipo con más captación de características de hardware.

- El respaldo de la información y configuración IOS de los equipos deberá ser almacenada en depósitos externos con fines de restauración inmediata ante reemplazo de equipamiento por daños severos o siniestros.

- Se recomienda además incorporar a la granja de servidores un equipo de servidor RADIUS el mismo que independizaría las conexiones para navegación visitante y a través de mecanismos de uso de VLAN independiente.

7 BIBLIOGRAFÍA

[1] Protocolo RADIUS. Estándar RFC2865 (2000). Sitio web: http://www.rfc-base.org/txt/rfc-2865.txt

[2] Tecnología de información-Técnica de seguridad-Código para la práctica de la gestión de la seguridad de la información. (2005). Norma ISO/IEC 17799

[3] Germán Alexis Cortes Hernández. (2014). Cálculo del ancho de banda (nominal vs efectivo). Abril, de TecnoSeguro.com Sitio web: https://www.tecnoseguro.com/analisis/cctv/calculo-del-ancho-de-banda-nominal-vs-efectivo.html

[4] Manuel Peñaloza Figueroa. (2007). Standard TIA-942. Septiembre, de UNSAAC-DAI Sitio web: https://profesores.ing.unab.cl/~delaf/archivos/cursos/topicos-de-especialidad/datacenters/material-de-apoyo/TIA-942/Dise%C3%B1o%20y%20Cableado%20de%20un%20Centro%20de%20Datos%20(TIA-942).pdf

[5] Obed E.H.R. (2010). Estándares TIA-EIA 568. Octubre, de Blog Sitio web: http://obedhr.blogspot.com/

[6] TELECOMMUNICATIONS INDUSTRY ASSOCIATION. (2001). TIA/EIA STANDARD. Abril, de ANSI Sitio web: http://nag.ru/goodies/tia/TIA-EIA-568-B.1.pdf

[7] JORGE ENRIQUE GUTIERREZ RICARDO. (2008). ESTUDIO DE FACTIBILIDAD PARA EL CONTROL DE ACCESO BIOMÉTRICO, EN UNA EMPRESA EMPLEANDO LECTORES DE HUELLA DIGITAL. ENERO, de UNIVERSIDAD DE LA SALLE Sitio web: http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1

[8] Calos Ivan Zuluga Vélez. (2013). NORMATIVIDAD Y TECNOLOGIA DE PROTECCIÓN DE INCENDIOS EN CENTROS DE COMPUTO Y TELECOMUNICACIONES. Noviembre, de GZ Ingenieria Sitio web: http://www.gzingenieria.com/pdf/

[9] ISO/IEC. (2009). INTERNATIONAL STANDARD ISO/IEC 11801. Octubre, de ISO/IEC Sitio web: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&sqi=2&ved=0ahUKEwiEtuHX6JHPAhVJkh4KHUqFDnEQFggtMAM&url=http%3A%2F%2Fiiti.it%2Fhome%2Findex.php%2FDownload-document%2F6-Generic-cabling-for-customer-premises.html&usg=AFQjCNH8vD5y-naevWtL9cXuD3cI6BIFVw&sig2=xTGBnRrVH33j9uaMeQZhKA&bvm=bv.132479545,d.dmo

[10] Enrique del Rio. (2012). Categorías utilizadas actualmente en instalaciones de cableado estructurado. Septiembre, de Dpto. Electrónica IEFPS Tartanga Erandio Bizkaia Sitio web: http://fibraoptica.blog.tartanga.net/2012/09/03/situacion-actual-de-las-categorias-de-cables-de-pares/

[11] Uyless D. Black. (1987). Redes de transmisión de datos y proceso distribuido. Madrid: Díaz de Santos S.A. Pág. 333

[12] Chris DiMinico. (2005). Telecommunications Infrastructure Standard for Data Centers ANSI/TIA-942. Noviembre, de IEEE Sitio web: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf

[13] Nicholas C. – Thomas A. (2006). Educación: Riesgos y Promesas de las nuevas tecnologías de la Información, Pág. 16-37

[14] Perspectivas sobre los riesgos de TI. Seguridad de la Información en un mundo sin fronteras, Erns & Young, sitio web: http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/%24FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf

[15] Redes cableadas, seguridad activa- VLANs. (2014), sitio web: https://infosegur.wordpress.com/tag/vlan/

[16] Alejandro Corletti Estrada. Madrid (2011). Seguridad por niveles, Sitio web: http://www.tic.udc.es/~nino/blog/lsi/documentos/seguridad-por-niveles.pdf

[17] Javier Areitio Bertolin. (2008). Seguridad de la información Redes Informáticas y Sistemas de Infamación. Madrid: Paraninfo