UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PROPUESTA DE SEGMENTACIÓN CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLANTA NORTE.

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

JULIO EDGAR MOLINA RUIZ

Chiclayo, junio de 2012

"PROPUESTA DE SEGMENTACIÓN CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO – PLANTA NORTE"

POR:

JULIO EDGAR MOLINA RUIZ

Presentada a la Facultad de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo.
Para optar el título de:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR EL JURADO INTEGRADO POR

_____

Ing. Héctor Miguel Zelada Valdivieso
PRESIDENTE

_____

Ing. Consuelo del Castillo Castro
SECRETARIO

_____

Ing. Gregorio Manuel León Tenorio
ASESOR

DEDICATORIA

A mis padres, Víctor Molina y María Sofía Ruíz, por su dedicación y sacrificio, ya que ambos fueron la motivación para convertirme en un profesional.

A Chío por su amor incondicional que día a día me brinda y que es la fortaleza en mi vida, orientándome y aconsejándome para ser mejor persona.

A mi amigo, Jorge Palomino por su apoyo en las etapas de mi formación académica, demostrándome el verdadero sentido de la amistad.

AGRADECIMIENTOS

A Dios, por manejar los hilos de mi vida y haberme permitido vencer los obstáculos en mi camino.

Al ingeniero Gregorio León Tenorio por la orientación profesional que me brindó en el desarrollo de este proyecto. A la Ing. María Arangurí por su tolerancia y marcar la pauta en la investigación. A la Ing. Jessie Bravo, por sus aportes y sugerencias.

A la Universidad Santo Toribio de Mogrovejo por ser la casa de estudios que ha permitido mi formación académica y haberme demostrado, que un buen profesional, no solo es un cúmulo de conocimientos sino también de valores.

ÍNDICE

RESUEN

El presente trabajo plantea una propuesta de Segmentación con Redes de Áreas Locales Virtuales (VLAN's) y priorización del Ancho de Banda con Calidad de Servicio (QoS) para la mejora del Rendimiento y Seguridad de la Red de Área Local (LAN) en la Empresa Editora El Comercio – Planta Norte.

La empresa Editora El Comercio – Planta Norte posee una red plana en su diseño lo cual dificulta la administración del tráfico de la Red, debido a la ausencia de estándares de calidad en gestión de tráfico LAN, políticas de seguridad no alineadas a las necesidades de la empresa y desaprovechamiento de la performance de los equipos de comunicación instalados.

Esto ha ocasionado la latencia de la red en horas pico, degradándose la velocidad de transferencia por el tráfico desmedido de la información y perjudicando o retardando los procesos más importantes en la empresa en intervalos de 60 a 90 minutos.

Asimismo, la información periodística enviada por los corresponsales hacia la Planta, ocasiona pérdida de tiempo en acciones de "subida" y "descarga" de archivos (Fotos, videos, infografías, avisos publicitarios, etc.). Adicionalmente, los parámetros de seguridad de la Red no garantizan la inviolabilidad de los equipos y la manipulación de la información, lo cual representa un riesgo para la integridad y desarrollo de los procesos.

Por ello, se rediseñó la red para el soporte de redes LAN Virtuales y de esta manera, segmentar las áreas en subredes para un mayor nivel de protección; brindar seguridad (Listas de Control de Acceso ACL's, Tecnologías emergentes en Seguridad Windows Server 20008, Nivel de autentificación – Radius); mejorar el consumo de Ancho de Banda (Calidad de Servicio QoS, Protocolo de Agregación de Enlaces de Control LACP, Troncales, etc.); implementar nuevos protocolos en tecnología CISCO; instalar redes inalámbricas y nuevos Servicios de transferencia de archivos (Protocolo de Transferencia de Archivos FTP)

Todo ello, con el propósito de disminuir costos y elevar la productividad de la Planta Norte, haciéndola más robusta y escalable ante un crecimiento tecnológico a mediano y largo plazo.

PALABRAS CLAVE

Red de Área Local , Redes de Áreas Locales Virtuales, Protocolo de Agregación de Enlaces de Control, Listas de Control de Acceso, Radius, Calidad de Servicio, Protocolo de Transferencia de Archivos

ABSTRACT

This work presents a proposal of Segmentation with Virtual Local Area Network (VLAN´s) and prioritization of bandwidth with Quality of Service (QoS) for improving Performance and the Security of the Local Area Network (LAN) in the El Comercio Publishing Company - North Plant.

El Comercio Publishing Company - North Plant has a flat network design which makes difficult the management of network traffic, due to the absence of quality standards in traffic management Lan, security policies are not aligned to the needs of the company and wastage of the development of communications equipament installed.

This has caused latency in the network during important hours, degrading the speed of transfer by the excessive traffic of the information and damaging the
Therefore, the journalistic information sent by correspondents of the company causes loss of time during the "upload" and "download" of the files (photos, videos, computer graphics, advertisements, etc.). Additionally, the security parameters of the network do not guarantee the inviolability of the equipment and manipulation of information, which represents a danger to the integrity and development of processes.

For that reason the network was redesigned for the support of the Virtual LAN nets, this allowed segmented the areas in subnets for a higher level of protection, provide security (Access Control Lists ACL's, Security Emerging Technologies in Windows Server 20008, Level Authentication - Radius); improve the consumption of bandwidth (Quality of Service QoS, Link Aggregation Protocol Control LACP, Trunk, etc.) implement new protocols on CISCO technology, install new wireless networks and new services and file transfer (File Transfer Protocol FTP).

All this, with the aim of reducing costs and increasing productivity of the company, and making it more robust and scalable in front of a technology growth to a medium or long term.

KEY WORDS

Local Area Network , Virtual Local Area Network, Link Aggregation Control Protocol, Access Control Lists, Radius, Quality of Service, File Transfer Protocol.

I. INTRODUCCIÓN

Es indudable el impacto social, económico y cultural que ha generado la tecnología en nuestros tiempos, donde cada vez la sociedad se vuelve más dependiente de esta, y es que, sus aportes al desarrollo humano hasta ahora son valorables.
Bajo este panorama, los negocios empresariales no son ajenos a su influencia y utilidad como herramienta de desarrollo y eficiencia. Hoy en día las computadoras, los software's, los protocolos y equipos de comunicación, deben estar correctamente implementados y configurados, de tal manera que, todos ellos trabajen de una forma armoniosa, maximizando así sus funciones de trabajo.
Desde un enfoque empresarial podemos decir que esta comunicación entre distintos dispositivos, equipos, personas, etc. se traduce en un gran sistema de redes, redes de datos que vienen siendo planificadas e instaladas de acuerdo a las necesidades de cada organización o empresa.
Sin embargo, el crecimiento experimentado en las empresas y en las actividades de negocios, ha motivado la expansión de las redes empresariales; aspecto que ha traído como consecuencia, la preocupación por los costos relacionados.
Ante esto, la Empresa Editora El Comercio - Planta Norte también experimenta cambios y debe adaptarse al crecimiento tecnológico, a la necesidad de crear nuevos procesos o mejorarlos, a potenciar la productividad con la misma cantidad de recursos, etc. Cambios que vienen afectando sus procesos, tareas y funciones y que, deben adaptarse rápidamente a los nuevos requerimientos de trabajo, todos ellos bajo el marco de la plataforma tecnológica que posee: La Red de Datos.
Por ello, nace la propuesta de la Segmentación de la Red de Datos con Redes Virtuales y la priorización del Ancho de Banda con QoS para mejorar así el Rendimiento y Seguridad de la Red LAN en la Empresa Editora El Comercio – Planta Norte.

La Empresa Editora el Comercio S.A. – Planta Norte, bajo el rubro de las Telecomunicaciones viene desarrollando sus actividades en Chiclayo desde hace cinco años. Inicialmente se concibió como una Planta con fines de impresión de los diarios, Perú 21 y Trome; encargándose de recibir las páginas digitales de los diarios en mención, diseñadas en la Planta Principal en la ciudad de Lima.

Debido a la gran demanda de estas publicaciones en la Región Nororiental, se decidió que los diarios Trome, Peru21, Depor, El Comercio y suplementos, se elaboren, procesen y diseñen en la Planta de Chiclayo, trayendo consigo la necesidad de la creación de nuevas áreas y por consiguiente, la instalación de nuevos módulos informáticos por área con la finalidad de brindar soporte a los flujos de información.
Esta convergencia de cambios, ocasionó un crecimiento de la capacidad de Producción del 10% a un 85% desde su°s inicios. Paralelo a ello, el crecimiento tecnológico en hardware, experimentó un aumento promedio de 16% anual, como equipos de cómputo, impresoras, Plotters, etc. (**Anexo I)**

Cuadro Nº 01: Evolución del crecimiento en hardware

Año	Nro. Equipos	Crecimiento respecto del año anterior (%)
2006	23	--
2007	28	22%
2008	35	25%
2009	40	14%
2010	45	12%
2011	50	11%

Promedio Crecimiento Anual = 16%

El crecimiento provocó que la plataforma LAN, tuviera congestionamiento en el tráfico de la Red (Degradación de la tasa de transferencia a 250 Kb/s) debido a envíos (Flujo Externo) y transferencias (Flujo Interno) de páginas periodísticas (50MB), imágenes (10MB), videos (250-500 MB), infografías (50MB -80 MB), etc. Considerando que la velocidad promedio con la que operaba la red, era de 3Mb/s. lo que afectaba la ejecución de diversos aplicativos, especialmente los de esquema Cliente/Servidor (ERP SAP, Arkitex, DTI, Excalibur Manager), Correos Electrónicos, Messenger, Print Plotter (Impresión en Plotter de paginas prediseñadas) y Comunicación Telefonía IP. **(Anexo II)**. Esto a su vez permitía percibir la necesidad de contar con señal inalámbrica para procesos transaccionales en el Sistema SAP.

Esta deficiencia era evidente en horas pico (5:00 p.m.– 9:00 p.m.) ocasionando malestar entre los 65 trabajadores de las diversas oficinas, lo cual traía consigo un promedio de demora que oscilaba entre una y una hora y media, perdiendo tiempo valioso en los procesos editoriales. **(Anexo V).**

Por esta razón, la hipótesis establecida para la presente investigación planteó el rediseño e implementación de tecnologías de redes que permitiera la Segmentación con Redes Virtuales y la priorización del Ancho de Banda con QoS para mejorar el Rendimiento y Seguridad de la Red LAN en la Empresa Editora El Comercio – Planta Norte.

En este sentido, se propuso el logro de los siguientes objetivos:

- Aumentar la escalabilidad en la red.

- Lograr que la velocidad o tasa de transferencia de datos esté dentro del rango aceptado como porcentaje del ancho de banda teórico y que en las horas pico no baje del mínimo permitido.

- Lograr la disponibilidad continua y permanente, 24 x 7 (24 horas al días, 7 días a la semana) de los servicios de Red (Correo electrónico, internet, aplicaciones, recursos compartidos)

- Incrementar tecnologías que permitan calidad de servicio.

- Reducir el número de eventos de pérdida de información.

- Aumentar el número de recursos de red compartidos con acceso administrado y controlado.

- Implementar mecanismos para autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario.

El presente estudio se fundamentó en las siguientes justificaciones:

En lo Social, en la medida que buscó generar un impacto positivo en la operación de los procesos, bajo ciertos estándares y parámetros preestablecidos, en aras de brindar un producto de calidad, con información veraz, objetiva y exclusiva. En lo tecnológico, pretendió mejorar la productividad de la red, haciendo uso de tecnologías, métodos y procedimientos que existen en el mercado, como el uso de técnicas de segmentación de la red para una mejor organización, implementación de directivas de seguridad interna y externa, uso planificado de los equipos informáticos, racionalizándose su utilización. Todo ello, sustentado en métodos y análisis, de acuerdo a la metodología Cisco.

En lo económico representó una inversión recuperable a mediano y largo plazo, que resultó beneficiosa en base a los resultados de la tecnología adquirida, logrando que los procesos del negocio culminen en el menor tiempo, lo que a su vez conllevó a que la cadena productiva se vea beneficiada con resultados económicos perceptibles, generando un impacto en la eficiencia y la productividad de la empresa.

II. MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

2.1.1. TESIS LOCALES

Titulo	SOLUCIÓN PARA EL SISTEMA DE COMUNICACIONES DIGITALES DE LA EMPRESA AGROINDUSTRIAL POMALCA S.A.
Autor	Samamé Villegas, Roberto Frank.
Año	Julio 2010
Universidad	Universidad Católica Santo Toribio de Mogrovejo.
Resumen	La presente investigación fue realizada con el objetivo de diseñar e implementar una Red Inalámbrica de área local (WLAN) para la Empresa Agroindustrial Pomalca a fin de mejorar la comunicación y el nivel de seguridad en la red de la empresa azucarera. Ello se logró contribuyendo a la existencia de una mayor cobertura de conexión para los trabajadores y permitió mayor dinámica dentro de los flujos de trabajo; apoyando a la cadena productiva y económica de la empresa. Todo ello sustentado en la investigación de optar por la mejor tecnología de acuerdo a la infraestructura y giro del negocio.
Correlación	La mencionada tesis está relacionada con el proyecto desarrollado, porque ambos proponen soluciones para la interconexión de las áreas y anexos de una empresa, basado en el Diseño de Redes y planeamiento estratégico en aras de una continua optimización. Si bien la técnica elegida en este proyecto para la interconexión no es aplicable al nuestro, dada las condiciones distintas pues aquí los puntos a interconectar pueden ser cubiertos por enlaces de antenas; pero sí podemos tomar en consideración los objetivos comunes perseguidos como: enlace permanente, seguridad y canal seguro de comunicación, priorización del ancho de banda jerarquizando el contenido a transferir, división de los dominios de broadcast para cada Red LAN Inalámbrica y control de acceso a los recursos.

Titulo	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE RED PARA MEJORAR EL SISTEMA DE COMUNICACIÓN EN EL PROYECTO ESPECIAL DE INFRAESTRUCTURA DE TRANSPORTE NACIONAL-PROVIAS NACIONAL-ZONAL II LAMBAYEQUE.
Autor	Cotrina Reaño, Oscar Alexander Guevara Flores, Liliana Arlita
Año	Octubre 2006
Universidad	Universidad Católica Santo Toribio de Mogrovejo.
Resumen	La tesis trata del Diseño e implementación de un sistema de red para mejorar el sistema de comunicación en el Proyecto Especial de Infraestructura de Transporte Nacional – PROVIAS NACIONAL, considerando las oficinas de su dependencia la ZONAL II LAMBAYEQUE, ubicadas en la avenida Santa Victoria N°719 –

	Chiclayo y las estaciones de peaje de Mocce y Mórrope, ubicadas en la Panamericana Norte, Ramal Nororiental y Ramal Norte, respectivamente. Se concluyó que el uso de VPN es un método de acceso seguro desde puntos externos a la red LAN, también se concluyó que la implementación de directivas de seguridad a través de Active Directory de Windows permitió desplegar las restricciones que se plantearon para un nivel de seguridad óptimo a nivel de usuario.
Correlación	Está relacionada con el proyecto en desarrollo, en la medida en que ambas establecen propuestas de solución y mejora en la conectividad de los distintos componentes del sistema de comunicación; todo ello apoyado en un Sistema de Red (LAN/WAN) y tecnologías de seguridad, performance y aplicación de un conjunto de software para monitorear su rendimiento. Ello permite que la propuesta desarrollada, tome como referencias algunas estrategias de éxito aplicadas en el antecedente, como el uso de VPN's y directivas de seguridad internas como Active Directory como instrumento de seguridad.

Titulo	"Implementación y Administración de una Intranet en la Red Asistencial Lambayeque de EsSalud.
Autor	Gonzales Rojas, Luis
Año	2006
Universidad	Universidad Señor de Sipán
Resumen	Esta tesis se basó en el uso de la tecnología como factor óptimo en la implementación de la Intranet dentro del sector salud, el uso de tecnologías de información y de las telecomunicaciones desde una perspectiva de modernización, destacando su importancia dentro del plan estratégico de la institución, con los cual se buscó solucionar un conjunto de deficiencias en el flujo de la información, como prolongados tiempos de espera, trámite documentario innecesario, información incompleta, etc. Por todo ello, la propuesta pretendió minimizar el impacto que genera toda esta problemática, factor común en muchas instituciones. Por ello su aportación es importante desde el punto de vista de un modelo a seguir para otras entidades del mismo rubro.
Correlación	La implementación de esta propuesta tecnológica, se relaciona en la medida que busca solucionar el problema que presenta la Red Asistencial Lambayeque de EsSalud, mediante el análisis previo del conjunto de deficiencias, tomando valores, y obteniendo la mejor alternativa de solución dentro de la plataforma de las Redes informáticas con soporte web. Si bien aquí se propone el uso de herramientas de administración de la red, no se ha evaluado el impacto de esta herramienta a nivel del uso de ancho de banda, tecnología de protocolos que estas herramientas usan como SNMP. Del mismo modo el presente proyecto se propone mejorar la

	plataforma tecnológica de las comunicaciones con la utilización de herramientas o aplicativos, Pilas de Protocolos de Red, Estándares de calidad en Lan's, Directivas de Seguridad todo ello con la premisa de atacar deficiencias tecnológicas en la empresa, que si bien son distintas por el giro del negocio, convergen en la medida que obstaculizan los procesos de la institución.

Titulo	Proyecto de Interconexión de Agencias Financieras Chiclayo-Tumán
Autor	Cotrina Orrego María Cecilia
Año	2005
Universidad	Universidad Nacional Pedro Ruiz Gallo.
Resumen	El proyecto analizó y diseñó la interconexión de las agencias financieras Cooperativa de Ahorro y Crédito Tumán con la agencia sucursal ubicada en el centro de la ciudad de Chiclayo, donde se propuso implementar una tecnología que sea segura y eficiente sin incurrir para ello en altos costos. El autor recomendó que es necesario dimensionar el requerimiento en función a los criterios de distancia a cubrir y servicios disponibles. Se concluyó que la interconexión de las agencias respondía a las exigencias del mercado y la competitividad, usando para ello, la tecnología como herramienta indispensable para el apoyo del plan estratégico de la empresa.
Correlación	La relación con nuestro estudio es que la realidad es similar en cuanto a interconectar oficinas o sucursales ubicadas en zonas alejadas además que para nuestro caso también necesitamos que la Red de Datos sea segura, eficiente y que logre reducir los costos en su administración y mantenimiento. El problema que se analiza en ambos estudios es similar, pero la solución es diferente; por tanto tenemos en cuenta las recomendaciones de dimensionar el requerimiento en base a distancia a cubrir y uso de redes alquiladas o dedicadas sobre Internet. Además se destaca el tema de la seguridad, factor que es decisivo por el giro del negocio.

Titulo	Análisis y Diseño para la implementación de la Red de Clínicas "Max Salud" departamento de Lambayeque.
Autor	Chau Loo Kung, Diana Carolina Sialer Rivera, María Noelia.
Año	2004
Universidad	Universidad Nacional Pedro Ruiz Gallo.

Resumen	En esta tesis se propuso que en las Clínicas y Oficinas de Max Salud se cuente con información actualizada, para ello se evidenció lo importante de la conexión entre locales, asumiendo que la conexión es del tipo 24x7 (24 horas al día, los 7 días de la semana), permitiendo un contacto ininterrumpido entre las diversas áreas y clínicas, aportando así una plataforma capaz de soportar futuras aplicaciones y así integrar procesos. En este caso se concluyó que los parámetros, para evaluar la alternativa a seleccionar, deben estar de acuerdo a las necesidades de la empresa, siendo para este caso: disponibilidad 7x24; fiabilidad de la información, seguridad y posibilidad de crecimiento (escalabilidad).
Correlación	Este estudio nos permitió tomar conciencia de la importancia de no disponer únicamente de un enlace físico para interconectar las oficinas en diferentes ubicaciones sino también de tener un enlace con ciertas características como la disponibilidad, fiabilidad, seguridad y escalabilidad; todas estas características deben ser tomadas en cuenta al momento de diseñar una red de datos, realizándose una estimación del ancho de banda en función a las características y requerimientos de las aplicaciones existentes como las que se proyectan implementar y utilizar.

Titulo	Diseño de Red Estructurada de Datos con VLan's aplicado en la Municipalidad Distrital de Puerto Eten.
Autor	Gonzales Vargas, Elmer
Año	2003
Universidad	Universidad Nacional Pedro Ruiz Gallo.
Resumen	Este estudio buscó incrementar la seguridad de datos y la información dentro de la red en la Municipalidad Distrital de Puerto Eten, proponiendo un mejor control en el Dominio Broadcast y la Gestión de la Red, sugiriendo la implementación de una Red Virtual Local para lograr este objetivo. Se demostró que la implementación de VLAN proporciona una serie de beneficios como: Segmentación de red, división y control del dominio broadcast, división lógica de una LAN basada en la estructura y nivel organizacional, seguridad a nivel de la capa de Red es decir a nivel IP.
Correlación	Este estudio respalda la utilización de VLan's para el diseño de una red de datos, demostrando su utilidad y eficacia para incrementar la productividad en una red LAN y cuyos beneficios son demostrados en este proyecto. También se destaca el papel importante y preponderante de la Seguridad y de las herramientas que se utiliza para lograrlo, detalle que hoy en día se ha vuelto prioridad y que obligan a las tecnologías estar en constante evolución, sirviendo así como guía para revalorar su importancia dentro de la empresa.

Titulo	Desarrollo del Proyecto de Tendido de Red de Alta Velocidad para la interconexión entre las diferentes facultades y dependencias de la Universidad Nacional Pedro Ruiz Gallo.
Autor	Llontop Cumpa, Luis Alberto Nicho Córdova, Ernesto Ludwin.
Año	2000
Universidad	Universidad Nacional Pedro Ruiz Gallo.
Resumen	El proyecto sugirió desarrollar un tendido de Red de alta velocidad, que permita interconectar las diferentes facultades y dependencias de la Universidad Nacional Pedro Ruiz Gallo, para así gestionar de manera eficiente la información que fluye entre ellas. También se describió y analizó las opciones de acuerdo a parámetros tecnológicos y económicos, aportando así tentativas de solución para la actualización tecnológica en la Universidad. Se concluyó que la estimación del ancho de banda debe estar en función al tipo de información a transferir y asignando una prioridad a cada una de ellas.
Correlación	Coincide en el propósito del uso de ciertos estándares en cuanto a tecnología para interconectar sobre una LAN extendida varios nodos, de tal forma de asegurar la disponibilidad del enlace y mantener una adecuada performance. Aquí tomamos en cuenta la experiencia en la determinación y estimación del ancho de banda ideal en función al tipo de información a transferir o compartir entre los puntos que se interconectan; en base a este ancho de banda y la necesidad de la disponibilidad de la red se selecciona la alternativa entre las diferentes tecnologías existentes. El criterio de priorizar el ancho de banda en función al tipo de información nos da la idea del uso de QoS.

2.1.2. TESIS NACIONALES

Titulo	Rediseño de la Red LAN del Hospital Belén de Trujillo.
Autor	De la Torre Battifora, Miguel Ángel
Año	2011
Universidad	Universidad César Vallejo.
Resumen	El proyecto tuvo como finalidad rediseñar la red LAN del hospital, partiendo de un análisis de la problemática actual, cuyos hechos más evidentes denotan una lentitud o latencia de la red, además de un cableado estructurado no estandarizado sin considerar los patrones de diseño mínimo. Se concluyó que para la implementación de una solución con VLAN es necesario que se asegure primero que a nivel

	físico (cableado + equipos activos + pasivos) se tenga un diseño de acuerdo a los parámetros.
Correlación	La correlación está en la similar situación problemática en que parten ambos trabajos, y se debe llegar a tener una situación final equivalente con una estandarización del cableado estructurado y los indicadores de evaluación del rendimiento de la red de acorde a lo generalmente aceptado y una evidente satisfacción de los usuarios. Para nuestro caso, el primer paso que se recomienda, se cumple por lo que es posible optar por la solución con VLAN.

Titulo	Diseño de la red LAN – campus
Autor	Guevara Julia, José Zulú
Año	2005
Universidad	Universidad Nacional Mayo de San Marcos
Resumen	Los objetivos del trabajo referido fueron reducir los costos operativos de la institución implementando un cableado estructurado para el campus y todas las sedes a nivel nacional. Considerando que la Universidad tiene proyectado crecer en infraestructura tanto física como tecnológica. Por ello los estudios de factibilidad, jugaron un papel importante dentro de la institución, puesto que ello pretende servir de modelo para los demás campus que no cuentan con plataformas modernas. La propuesta estuvo apoyada bajo los últimos estándares tecnológicos del mercado.
Correlación	En este referido trabajo se trató de reducir costos operativos de la institución y a su vez compartir información y recursos entre las unidades orgánicas de la institución usando la plataforma tecnológica de comunicación (redes LAN). La investigación previa es sumamente importante, puesto que destaca el presente de la LAN y una mejora en un mañana de acuerdo a las herramientas y plataformas que hoy la tecnología brinda, haciendo énfasis en el uso de Dominios, GPO's, aplicativos de acceso a internet como Isa Server, proxys, etc.

2.1.3. TESIS INTERNACIONALES

Titulo	Rediseño de la red Lan del Hospital Eugenio Espejo para soporte de videoconferencia y diseño de la red de interconexión con hospitales de la ciudad de Quito
Autor	Olipa Buendía, Yenny Cristina Yupanqui Cushicondor, Isabel Cristina
Año	2011
Universidad	Escuela Politécnica Nacional de Quito
Resumen	Se planteó el rediseño de la red LAN del Hospital Eugenio Espejo para soporte de videoconferencia, por ello se presenta la situación actual de la red LAN, tanto en la parte pasiva como activa de la red; el análisis de tráfico de la red, las políticas de administración y seguridad con la que actualmente trabajan. Una de las conclusiones que se mencionaron hace referencia a que en el rediseño se priorizó el tipo de información crítica, que para este caso fue video y voz. El tipo de información tuvo que tener prioridad sobre el ancho de banda; para lograr esto se implementó QoS en todos los equipos activos.
Correlación	Existe un análisis comparativo de los equipos disponibles en el mercado con sus respectivos costos, procediendo a seleccionar la mejor alternativa. Aquí se muestra como implementar QoS en equipos CISCO, además de todas las consideraciones a tener en cuenta para aprovechar eficientemente el ancho de banda.

Titulo	DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL PARA LA EMPRESA ELÉCTRICA QUITO S.A., MATRIZ LAS CASAS, PARA LA TRANSMISIÓN DE DATOS Y VOZ SOBRE IP
Autor	PABLO ANDRÉS DÍAZ ALVEAR
Año	2010
Universidad	ESCUELA POLITÉCNICA NACIONAL – QUITO
Resumen	En esta investigación se concluyó que la implementación de VLAN es una solución para cubrir las necesidades más urgentes en el aspecto de comunicación-seguridad en la red de datos de la Empresa Eléctrica Quito S.A. (E.E.Q.S.A.); además esta solución se encuentra en el dominio del modelo de referencia TCP/IP. Además de solucionar las necesidades o requerimientos, se determinó que las VLan's también son una solución para lo planificado y proyectado de tener soluciones a las futuras necesidades y aplicaciones que ingresen y sean parte de la red de datos, como por ejemplo las aplicaciones multimedia (VoIP, Telefonía IP, Videoconferencia, etc.).

Correlación	La tesis está relacionada en la medida que ambas ofrecen soluciones en base a la implementación de VLan's además nos da una idea de que se podría hacer un símil con la tecnología QoS, pues como se demuestra en el estudio, se hicieron o segmentaron las VLAN en función a grupos de necesidades es decir, grupos que compartían mismo tipo de información multimedia. Esto nos otorga una alternativa adicional a tomar en cuenta para optimizar el rendimiento de una red, priorizando el tipo de información.

Titulo	Diseño y Evaluación del Tráfico de una Red LAN para la empresa SERVTEC S.A
Autor	Ana Cristina Guzmán
Año	2010
Universidad	ESCUELA POLITÉCNICA NACIONAL – QUITO
Resumen	Este proyecto contempló una solución de Diseño e implementación de una red LAN en un sistema de comunicaciones que garantice las aplicaciones de voz y datos de forma confiable y eficiente para el transporte de información. Se concluyó que de acuerdo a cada una de las actividades o servicios que ejerce cada uno de los departamentos, se puede realizar el análisis del respectivo dimensionamiento del tráfico que circulará por toda la red LAN; considerando así la velocidad efectiva promedio de las aplicaciones con respecto al correo electrónico, acceso a Internet, tráfico del servidor de datos, local, para los plotters, impresora y entre los departamentos.
Correlación	La tesis está relacionada en los métodos utilizados para cuantificar los indicadores de rendimiento de una Red LAN. Este proyecto representó un aporte importante para nuestro estudio porque nos otorgó formas y métodos para analizar el tráfico de red , además de la forma de dimensionar el tráfico de la red.

Titulo	Análisis de Tráfico de una Red Local Universitaria
Autor	Carina Vaca
Año	2010
Universidad	ESCUELA POLITÉCNICA NACIONAL – QUITO
Resumen	El propósito del trabajo fue analizar el tráfico de una red local universitaria (DICC), mediante un software comercial, Tracer Plus Ethernet, se estudió el flujo de información generado por los sistemas administrativos y académicos de la universidad. El tráfico fue monitoreado a nivel de las capas 2 y 3 del modelo OSI. El desempeño de la red se caracterizó mediante los parámetros Cantidad de Tráfico, Tasa de Transferencia y el Porcentaje de

	Utilización. Se determinó que la red universitaria, bajo la estructura actual, tiene un comportamiento dentro de los estándares recomendados.
Correlación	Este estudio nos da pautas para cuantificar la realidad problemática así como la obtención de resultados. Dentro de las recomendaciones, sugiere realizar un rediseño para mejorar la eficiencia del tráfico LAN, considerando la implementación de nuevos servicios. Esto hace posible que el tráfico generado circule de manera óptima aun con las nuevas aplicaciones implementadas. Paralelamente, la aplicación de políticas de calidad de servicio o de clasificación del tráfico, permitirán dar prioridad a la data sensible.

Titulo	Análisis de Tráfico de Red del Servicio de Administración Aduanera del Estado de Zulia – Venezuela
Autor	Yeraldi C. Rivero G.
Año	2010
Universidad	Universidad Rafael Belloso Chacín. Venezuela
Resumen	El propósito de la investigación fue realizar un análisis de tráfico de red del servicio de la administración aduanera del estado de Zulia, con la finalidad de proporcionar a los investigadores una herramienta teórica que permita determinar el comportamiento LAN bajo ciertos parámetros de cualquier red (velocidad de conexión, ancho de banda, tasa de transmisión, entre otros), a fin de proponer recomendaciones que permitan incrementar la calidad de servicio. El estudio fue descriptivo y de campo, con diseño no experimental transaccional descriptivo.
Correlación	En lo relacionado con las recomendaciones aportadas a tal situación se logra mencionar que se debe evaluar constantemente el nivel de tráfico existente en la red, adquirir tecnologías de software analizadores de red de última generación, se recomienda el análisis de otros parámetros para la medición del tráfico, valorar constantemente la plataforma tecnológica en cuanto a su configuración, instalación, modernización y aplicación para optimizar el funcionamiento de la red.

Titulo	Evaluación de la Calidad de los Servicios en Redes E-MAN
Autor	Eduardo de la Cruz Gómez; Félix F. Álvarez Paliza
Año	2006
Universidad	Instituto Tecnológico de Acapulco. México. Acapulco
Resumen	Aquí se concluyó que, Ethernet, al evolucionar a través del tiempo, ha presentado la necesidad de un mejor desempeño en el tráfico de datos; propuestas como la implementación del protocolo 802.1p ofrecen hasta cierta medida un control de la calidad de los servicios (QoS), pero al crecer la red Ethernet a ambientes metropolitanos (e-man), surgen nuevos retos de mayor conectividad y velocidad de transmisión, donde propone seguir investigando nuevos paradigmas en cuanto a tecnologías de redes se refiere.
Correlación	En el referido trabajo se evaluaron los parámetros de desempeño necesarios para caracterizar la red e-man, y se analizó un nuevo procedimiento para abordar los problemas de la calidad de los servicios; este trabajo también analiza el comportamiento del desempeño de un modelo de simulación basado en el núcleo de backbone de una red.

Titulo	Rediseño de la Red LAN de la Cruz Roja ecuatoriana sede central
Autor	López Véliz, Paul Alexander Naula Narváez, Fernando Ramiro
Año	2006
Universidad	Escuela Politécnica Nacional de Quito
Resumen	Este trabajo planteó el estudio y diseño de un prototipo de una nueva red de datos LAN para Cruz Roja Ecuatoriana Sede Central que debe mejorar el rendimiento de la misma, se realizó un enfoque de los aspectos teóricos necesarios para el desarrollo de éste trabajo, se trabajó sobre el análisis de la situación actual de la red, aspectos como componentes de hardware (cableado estructurado, equipos de comunicación, servidores, estaciones de trabajo), aplicaciones y servicios, análisis del tráfico de red. Entre sus conclusiones se mencionó que la tecnología VLAN es una forma de lograr una segmentación de la red a nivel lógico y además se consigue 2 objetivos: mejorar el rendimiento general de la red LAN y conseguir fortalecer la seguridad de la Red.
Correlación	Su relación con nuestra propuesta de diseño es el prototipo de una nueva red en base a la información recopilada, además parte fundamental de este estudio es la definición VLANS como alternativa de segmentación de la red. En el desarrollo del estudio se demostró que la implementación de VLAN es una alternativa segura y eficiente para incrementar la productividad y rendimiento de la Red LAN.

Titulo	"Metodología para el diseño de área local"
Autor	Alberto José Fernando Marroquín Piloña
Año	2002
Universidad	Facultad de ingeniería de sistemas, informática, y ciencias de la computación. Universidad francisco Marroquín (Guatemala)
Resumen	En la actualidad las redes de computadoras son de vital importancia para la vida de cualquier profesional, más aun de quienes están ligados a la tecnología y que de forma directa se encuentran involucrados en tareas de implementar redes de datos. Se ve la necesidad de elaborar una metodología, dado que la problemática en redes se debe a un diseño débil y mal estructurado que repercute en pérdidas económicas.
Correlación	Ambos trabajos persiguen el mismo propósito principal que es dar a conocer un enfoque que permita de manera adecuada, realizar la tarea de diseñar una red, tomando las consideraciones necesarias a seguir para la elaboración de un diseño robusto y sólido pero a la vez práctico y de fácil mantenimiento.

Titulo	Reingeniería y Optimización de la Red de voz y datos de Petrocomercial – Regional Norte
Autor	Rivadeneira Erazo, Alex Homero
Año	2005
Universidad	Escuela Politécnica del Ejército del Ecuador – Facultad de Ingeniería Electrónica
Resumen	Este proyecto tuvo por objetivo mejorar el desempeño de las principales redes locales de la Regional Norte de PETROCOMERCIAL, por medio del rediseño de redes y el diseño de redes de área local virtuales (VLan's), en base a las circunstancias, necesidades y disponibilidad de equipos de la empresa. A través de los objetivos, se consigue que las redes locales seleccionadas, obtengan flexibilidad y escalabilidad a través de una fácil administración, y además la factibilidad de seguridad en estas redes. También se mejora la calidad de voz sobre IP, debido a que a éste tráfico se le asigna su propia red virtual y una prioridad superior con respecto al tráfico de datos.
Correlación	La relación con nuestro estudio está en el objetivo de mejorar el servicio de telefonía IP dentro de las redes locales de la Planta Norte. Lógicamente mejorar los canales de transmisión dentro de la Lan, involucra administrar los paquetes de datos, colas de espera gestionadas por los switches, políticas de seguridad, etc, lo que repercutirá directamente sobre el rendimiento de la Lan, en relación a la telefonía IP de la empresa.

2.2. Bases Teórico-Científicas

2.2.1. Conceptos generales

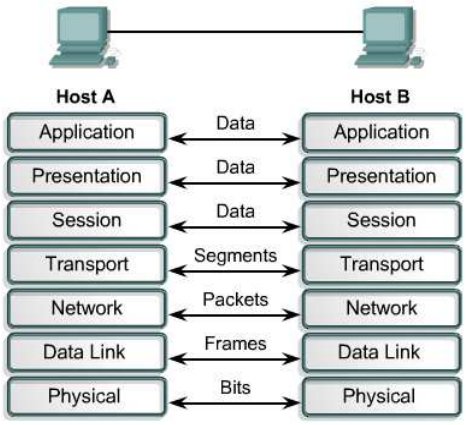
Modelo OSI

Open Systems Interconnection (1984): Es un modelo de red descriptivo de siete capas definido por la ISO, que asegura compatibilidad e interoperabilidad entre varias tecnologías de red producidas por diferentes compañías, lo que permite trabajar de manera independiente sobre funciones de red separadas y por ende disminuir su complejidad y acelerar su evolución.
Este modelo está formado por siete capas, cada una de las cuales realiza funciones diferentes, que son:

1. **Capa Física:** Especifica voltajes, conectores, tasas de transmisión, medios de transmisión, etc.
2. **Capa de Enlace de Datos:** Utiliza las direcciones MAC para acceder a las estaciones finales, notifica errores pero no los corrige, etc.
3. **Capa de Red:** Determina el mejor camino, utilizando direccionamiento lógico (IP).
4. **Capa de Transporte:** Provee una confiable o no confiable entrega de datos, reensambla los segmentos que llegan en desorden, etc.
5. **Capa de Sesión**: Establece, maneja y termina sesiones entre aplicaciones, asigna puertos lógicos, etc.
6. **Capa de Presentación:** Traduce entre varios formatos de datos, encriptamiento, compresión, etc.
7. **7) Capa de Aplicación:** Provee protocolos y software al servicio del usuario (Navegadores WEB, correo electrónico, etc.).

Para que los datos viajen desde un origen a su destino, cada capa del modelo OSI en el origen debe comunicarse con su respectiva capa en el destino. Esta comunicación es conocida como peer-to-peer. Durante este proceso, los protocolos de cada capa intercambian información denominada Protocol Data United (PDUs).

Figura Nº 01: Comunicación Peer-to-Peer



Fuente: http://www.vanguardms.com/documentation

Encapsulación, es el método que añade cabeceras y *trailers* a los datos que se mueven hacia abajo de la pila de capas del Modelo OSI. El dispositivo receptor desnuda la cabecera, que contiene direcciones para esa capa (desencapsulación).

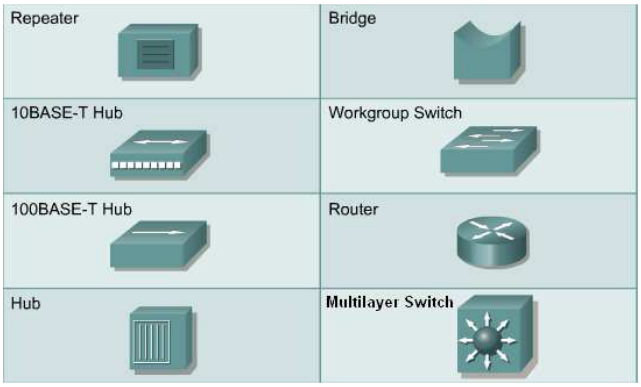
Es indudable que el Modelo OSI, marcó una referencia; que debe hacer cada componente de la red sin entrar en detalles de implementación, por ello se ha convertido en un estándar internacional y sirve como guía para la conectividad en red. Aunque existen otros modelos, en la actualidad la mayoría de fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando enseñan a los usuarios cómo utilizar sus productos, siendo así un marco para poder comprender de cómo viaja la información a través de la red.

2.2.2. Dispositivos de Red

William Stallings (2000). Señala que existen dos clasificaciones, la primera clasificación son los **dispositivos de usuario final**, como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario.
Estos dispositivos son conectados físicamente a la red usando una *Network Interface Card* (NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

Los **dispositivos de red** proveen la comunicación entre dispositivos de usuario final. Como por ejemplo:

Figura Nº 02: Iconos de los Dispositivos de Red



Fuente: http://www.cisco.com/web/learning/netacad

2.2.2.1. Repetidor

Es un dispositivo de red usado para regenerar una señal. Regeneran señales analógicas o digitales distorsionadas por la pérdida de transmisión debido a la atenuación. Es un dispositivo de capa 1.

2.2.2.2. Hub

Dispositivo de capa 1 que permite la concentración de varios dispositivos dentro de un solo dominio de colisión o segmento. Regenera y amplifica las señales de datos para todos los dispositivos conectados, excepto para el dispositivo que originalmente envió la señal. También es conocido como un repetidor multipuerto, que extiende los dominios de colisión.

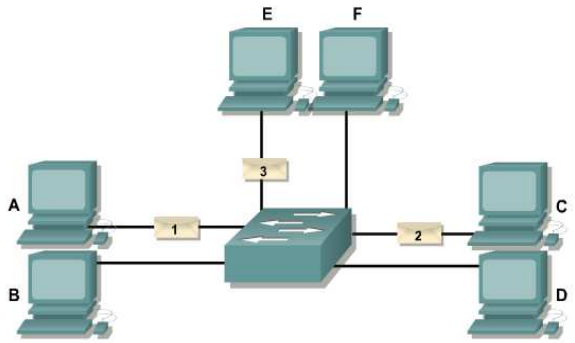
2.2.2.3. Bridge

Es un dispositivo de capa 2 que separa dominios de colisión, porque analiza las direcciones MAC para determinar si las tramas de datos pueden o no cruzar entre dos segmentos de red. Para lograr esto, el bridge aprende las direcciones MAC de los dispositivos en cada segmento conectado. Además este dispositivo puede convertir formatos de transmisión de datos, lo cual no puede realizar un switch de capa 2.

2.2.2.4. Switch

Andrew s. Tanenbaum- 4ta. Ed. (2003). Menciona que es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de las trama de datos transmitidas. Los switches aprenden las direcciones MAC de los dispositivos conectados a cada puerto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la CAM. Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos. Esto crea un ambiente libre de colisiones entre el origen y el destino lo cual implica la máxima utilización del ancho de banda disponible.

Figura Nº 03: Transmisiones Simultáneas en un Switch



Fuente: http://www.cisco.com/web/learning/netacad

Cada puerto del switch representa un solo dominio de colisión, lo cual se conoce como microsegmentación. La desventaja de todos los dispositivos de capa 2, es que ellos envían tramas broadcast a todos los dispositivos conectados a sus puertos.

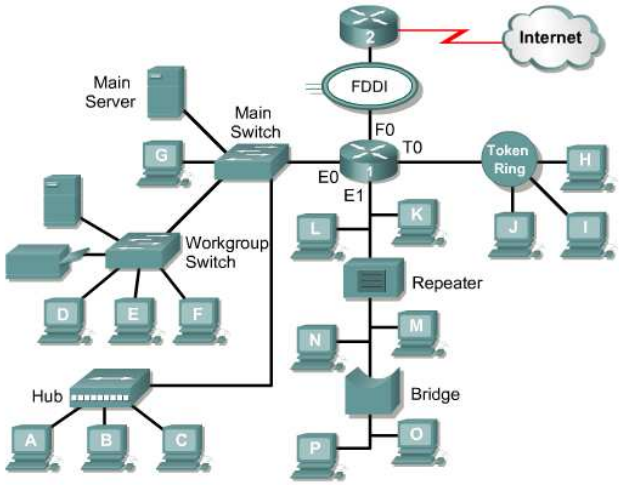
2.2.2.5. Router

Cisco Networkers Solutions Forum (2006). Se define como dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de enrutamiento para almacenar estas direcciones de capa 3. Los routers se encargan de elegir el mejor camino para enviar los datos a su destino y conmutar o enrutar los paquetes al puerto de salida adecuado.

Los routers dividen tanto dominios de broadcast como dominios de colisión. Además, son los dispositivos de mayor importancia para regular el tráfico, porque proveen políticas adicionales para la administración de la red con filtrado de paquetes para la seguridad.

También dan acceso a redes de área amplia (Wan), las cuales están destinadas a comunicar o enlazar redes de área local (Lan's) que se encuentran separadas por grandes distancias.

Figura Nº 04: Ejemplo de la Interconexión de Dispositivos de Red



Fuente: http://www.cisco.com

2.2.2.6. Switch multilayer

Un switch multilayer es la combinación de la conmutación tradicional de capa 2 con la operación de enrutamiento de capa 3 en un solo dispositivo, mediante acciones de hardware de alta velocidad. En tanto que en un router el enrutamiento se realiza mediante técnicas de software lentas. Este Switch se fundamenta en circuitos del tipo **ASIC**.

Los switches multilayer son más rápidos y baratos que los routers. Aunque algunos switches multilayer carecen de modularidad y flexibilidad que usualmente tienen asociados los routers.

En la actualidad existen switches que pueden manejar información relacionada desde la capa 2 (enlace de datos) hasta la capa 7 (aplicación) del modelo OSI.

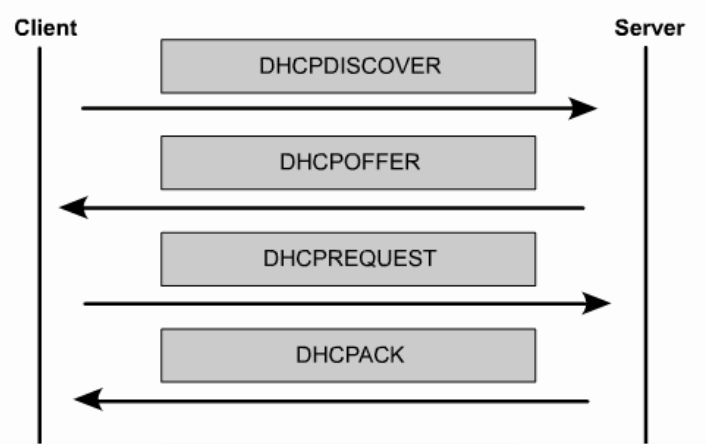
2.2.3. Protocolo de Configuración de Hosts Dinámico - DHCP

El DHCP (Protocolo de Configuración de Hosts Dinámico) *se basa en el* RFC 2131, y trabaja en modo cliente – servidor. El protocolo de configuración de hosts dinámico, habilita a los clientes DHCP, obtener sus configuraciones desde un servidor DHCP, considerando que la opción de configuración de mayor importancia, es la dirección IP asignada al cliente.

El DHCP no se utiliza para la configuración de los switches, routers o servidores. Estos hosts necesitan tener direcciones estáticas.

DHCP usa el UDP como protocolo de transporte. El cliente envía mensajes al servidor sobre el puerto 67, mientras que el servidor envía mensajes al cliente sobre el puerto 68. Los clientes DHCP arriendan la información del servidor por un periodo definido administrativamente. Y cuando el arrendamiento expira, el cliente debe pedir otra dirección, aunque generalmente se le reasigna la misma.

Figura Nº 05: Orden de la Transmisión de Mensajes DHCP



Fuente: http://www.cisco.com/web/learning/netacad

2.2.4. Ethernet

Ethernet o su estándar equivalente IEEE 802.3, es básicamente una tecnología de transmisión Broadcast, donde los dispositivos como computadoras, impresoras, servidores de archivos, etc.; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto, las colisiones son una natural ocurrencia en redes Ethernet y pueden llegar a ser un gran problema.

La entrega de tramas de datos Ethernet es de de naturaleza Broadcast. Ethernet usa el método CSMA/CD (Acceso Múltiple Sensible a Portadora con Detección de Colisión), que le permite a una sola estación transmitir, y puede soportar tasas de transmisión de alta Carrier Sense Multiple Access / Collision Detection velocidad, como: Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps y 10-Gigabit Ethernet: 10,000 Mbps.

El desempeño de un medio compartido Ethernet/802.3 puede ser negativamente afectado por factores como: las aplicaciones multimedia con alta demanda de ancho de banda tales como video e Internet, que junto con la naturaleza broadcast de Ethernet, pueden crear congestión en la red; y la latencia normal que adquieren las tramas por viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NICs.

2.2.5. Dominio de Colisión

Es un grupo de dispositivos conectados al mismo medio físico, es decir si dos dispositivos acceden al mismo tiempo al medio, entonces esto resulta en una colisión. Este es un dominio de capa 1.

2.2.6. Dominio de Broadcast

Es un grupo de dispositivos sobre la red que reciben mensajes de broadcast. Este es un dominio de capa 2.

2.2.7. Broadcast y Multicast

Para comunicarse con todos los dominios de colisión, los protocolos usan tramas broadcast y multicast en la capa 2 del modelo OSI. Por lo tanto si un nodo necesita comunicarse con todos los hosts en la red, éste envía una trama broadcast con una dirección MAC de destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual todas las tarjetas NIC deben responder.

La acumulación de tráfico broadcast y multicast de cada dispositivo de la red es referido como: **radiación de broadcast,** cuya circulación puede saturar la red, es decir que no hay ancho de banda disponible para aplicaciones de datos, resultando en la caída de estas conexiones, situación conocida como una **tormenta de broadcast.**

2.2.7.1. Causas de Broadcast y Multicast

Existen varias fuentes de broadcast y multicast en redes IP, estas pueden ser: las estaciones de trabajo, los routers, las aplicaciones multicast, el protocolo DHCP, etc. Las estaciones de trabajo envían broadcast de pedidos ARP (Protocolo de Resolución de Direcciones), cada vez que ellos necesitan localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast pueden ser causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho. Las aplicaciones multicast, particularmente las aplicaciones de paquetes de video pueden generar una cadena de siete megabytes de datos multicast, que en una red conmutada podría ser enviada a cada segmento, resultando en una severa congestión.

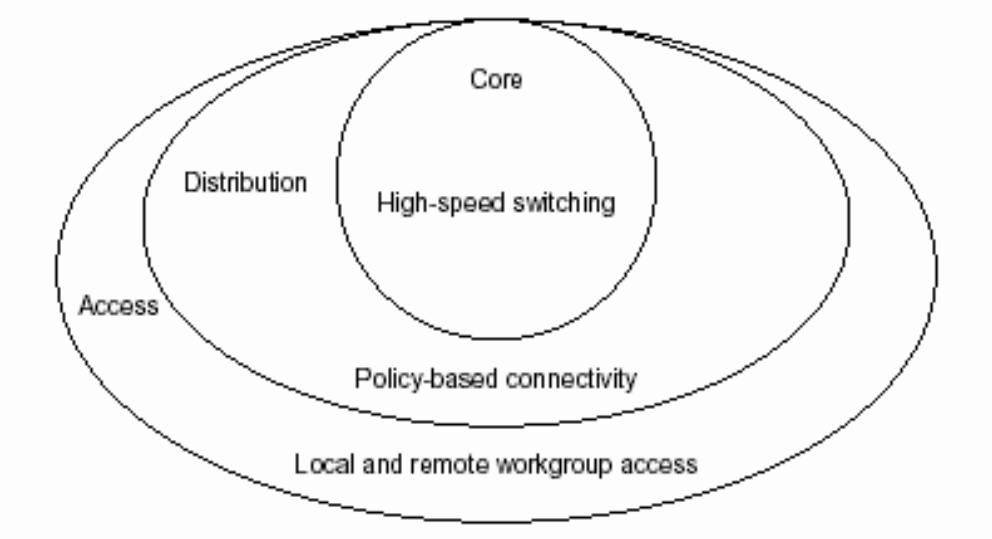
Otra fuente generadora de broadcast es el protocolo DHCP cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Además estos clientes por lo general repiten este pedido después de un relativo corto "timeout", posiblemente debido a una respuesta lenta del servidor, lo que producen las conocidas **tormentas de broadcast;** que a su vez producen retardos anormales de otros tráficos cliente / servidor, los cuales también pueden empezar a retransmitir.

2.2.8. MODELO JERÁRQUICO CISCO

Consta de tres capas:

- Capa Núcleo: **Backbone**
- Capa de Distribución: **Routing**
- Capa de Acceso: **Switching**

Figura Nº 06: Capas del Modelo Jerárquico Cisco



Fuente: www.redesymas.org

2.2.8.1. Capa Núcleo

Es el backbone de conmutación de alta velocidad que debe ser diseñado para conmutar paquetes lo más rápido posible, es decir es responsable del transporte de grandes cantidades de tráfico en forma confiable y rápida, por lo tanto la preocupación de esta capa es la velocidad y latencia. Es importante considerar, lo que no debemos hacer en esta capa:

- No realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, lo cual reducirá el tráfico.
- No soporta accesos de grupo de trabajo.
- Evitar expandir el núcleo o *core* cuando la red crece. Si el desempeño es un problema en el *core*, son preferibles las actualizaciones en lugar de las expansiones.

2.2.8.2. Capa de Distribución

También conocida como "*workgroup layer*", y es el punto de comunicación entre la capa de acceso y el *core*. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y determinar cómo los paquetes pueden acceder al *core* si es necesario.

La capa de distribución es donde se implementan las políticas para la red. Existen algunas acciones que generalmente deben hacerse en esta capa:

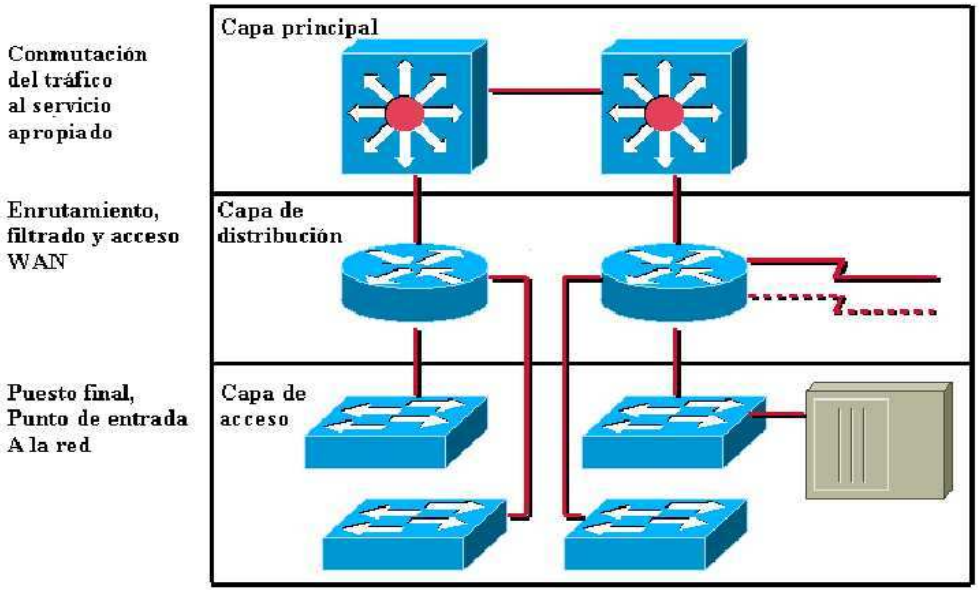
- Enrutamiento.
- Implementación de listas de control de acceso o filtro de paquetes.
- Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls.
- Calidad de Servicio, en base a las políticas definidas.
- Redistribución entre protocolos de enrutamiento, incluyendo rutas estáticas.
- Enrutamiento entre VLan's y otras funciones que soportan los grupos de trabajo.
- Definición de dominios de Broadcast y multicast.
- Posible punto para acceso remoto.
- Traslado de medios de comunicación.

2.2.8.3. Capa de Acceso

La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios. Los recursos de red de la mayoría de usuarios deben estar disponibles localmente. Esta capa también es conocida como "*desktop layer*". Estas son algunas de las funciones que incluye esta capa:

- Continúa el control de acceso y políticas (desde la capa de distribución)
- Creación de dominios de colisión separados (micro-segmentación)
- Conectividad de los grupos de trabajo dentro de la capa de distribución.
- Habilitar filtros de direcciones MAC.
- También es posible tener acceso a grupos de trabajo remotos.
- Presta servicios de asignación de VLANs a nivel de capa 2 del modelo OSI.

Figura Nº 07: Estructura de Red definido por Jerarquía

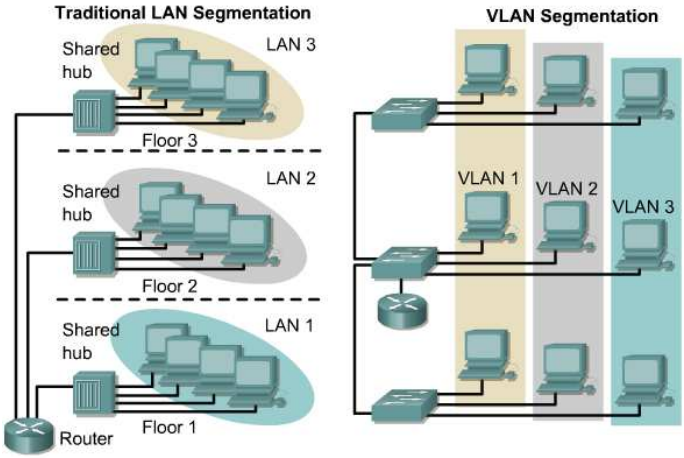


Fuente: www.geocities.ws

2.2.9. RED DE AREA LOCAL VIRTUAL

Una VLAN (Red de Área Local Virtual) es una agrupación lógica de dispositivos o servicios de red, en base a funciones, departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red.

Figura Nº 08: VLan's y Límites Físicos



Fuente: http://www.cisco.com

La función de las VLan's es una segmentación lógica de la red en diferentes dominios de broadcast, es decir que los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN.

Así como solo los routers proveen conectividad entre diferentes segmentos LAN, también solo los routers o

equipos que operen en la capa tres del modelo OSI, proveen conectividad entre diferentes segmentos VLAN. Los routers en topologías VLAN proveen filtrado de broadcast, seguridad y administración del flujo de tráfico.

2.2.9.1. Ventajas de las VLAN's

- **Incrementan el desempeño de la red** agrupando estaciones de trabajo, recursos y servidores según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN. (Mejor desempeño, facilidad de administración).
- **Facilidad en la administración** de adición, movimiento y cambio de estaciones de trabajo en la red. (Flexibilidad, Escalabilidad, Facilidad de Administración).
- **Mejoran la seguridad de la red**, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente (sin enrutamiento).
- **Incrementan el número de dominios de broadcast** mientras éstos decrecen en su tamaño. (Mejor desempeño).
- **Facilitan el control de flujo de tráfico**, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un Switch.(Mejor desempeño).
- La configuración o reconfiguración de VLan's se realiza a través de software, por lo tanto esto no requiere de movimientos o conexiones físicas de los equipos de red. **(**Facilidad de Administración).

Las VLan's proveen flexibilidad, escalabilidad, seguridad, facilidad de administración y mejor desempeño de la red.

2.2.9.2. Características de las VLan's

a.- VLAN de rango normal

- Para redes de pequeñas y medianas empresa.
- ID de VLAN entre 1 y 1005.
- ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI, estas VLAN se crean automáticamente y no se pueden eliminar. Las configuraciones se

almacenan en la valn.dat, el cual se encuentra en la memoria flash del switch VTP, solo puede asimilar VLAN de rango normal.

b.- VLAN de rango extendido

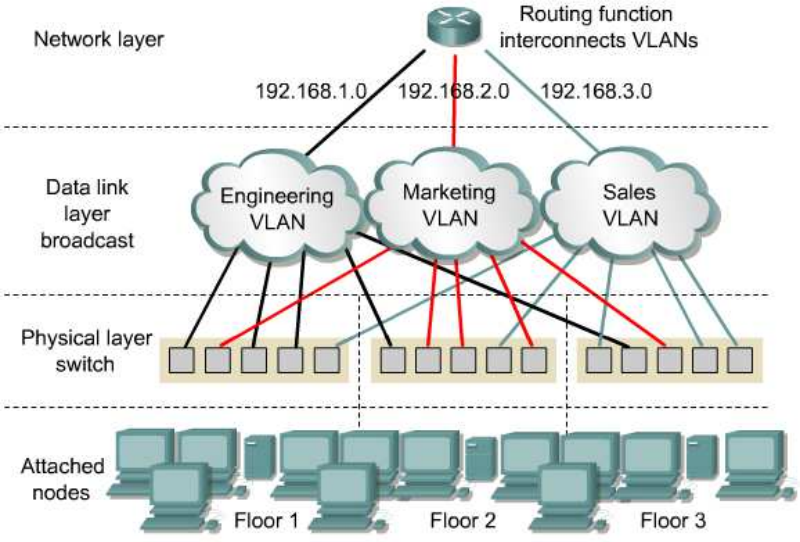
- Se diseñan para proveedores de servicios.
- ID de VLAN entre 1006 y 4094. Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución.
- VTP no aprende las VLAN de rango extendido.

2.2.9.3. Tipo de VLAN

a.- VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador, cuyas ventajas son:

- Facilidad de movimientos y cambios.
- Micro segmentación y reducción de dominio de broadcast.
- Multiprotocolo: la definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuando a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

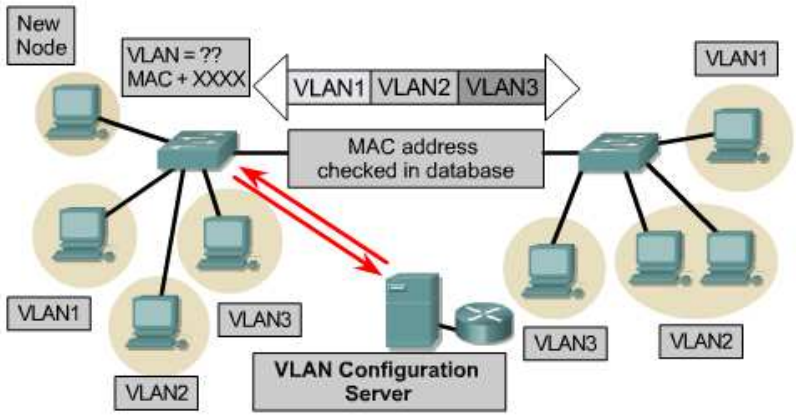
Figura Nº 09: VLan's en base a Puertos



Fuente: http://www.cisco.com/web/learning/netacad

b.- VLAN de nivel 2 (Denominada Vlan en base a Direcciones MAC) Operan agrupando estaciones finales a una VLAN en base a sus direcciones MAC. La forma cómo se realiza la asignación de usuarios a una VLAN es utilizando un servidor de políticas de administración de VLan's (VMPS), para que maneje la base de datos de todas las direcciones MAC; de tal forma que cuando un usuario se conecte a un puerto de un Switch, éste último, consulte al servidor a que VLAN corresponde este dispositivo, de acuerdo a su dirección MAC.

Figura Nº 10: VLan's en base a Direcciones MAC



Fuente: http://www.cisco.com/web/learning/netacad

También permite a los administradores de red mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. Por lo tanto las VLan's basadas en MAC prestan su mayor servicio de movilidad y seguridad a nivel de computadoras portátiles.

La principal desventaja, es que inicialmente se necesita recopilar la información de las direcciones MAC de todas las estaciones de trabajo de la red, para construir la base de datos que necesita el servidor de políticas.

2.2.9.4. Estándar

Las VLAN están definidas por el estándar:

802.1Q: El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el

nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

2.2.9.5. Etiquetado de la Trama 802.1Q

La norma IEEE 802.1Q identifica el mecanismo de etiquetado de trama de capa 2. El protocolo 802.1Q interconecta switches, routers y servidores. Solo los puertos FastEthernet y GigabitEthernet soporta el enlace troncal con el etiquetado 802.1Q (tambien conocido como Dot1q). Gracias a este protocolo los switches reconocen la existencia de VLANS a través del etiquetado de trama, reconociendo el número de VLAN independientemente del nombre que estas VLAN posean en cada switch.

- Los Switch solo utilizan la información del encabezado de trama para enviar paquetes.El encabezado no contiene la información que indique a que VLAN pertenece la trama.
- Cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen.
- Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.
- Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

2.2.9.6. Estándares integrados

- IEEE 802.1p: Es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).802.1p está integrado en los estándares IEEE 802.1D y 802.1Q.

- IEEE 802.10: El protocolo Inter-Switch de Cisco (ISL) para VLANs en Ethernet y tecnologías similares del LAN fue basado en IEEE 802.10; en este uso 802.10 ha

sido substituido en gran parte por IEEE 802.1Q.

- IEEE 802.1D: Las VLANs (redes virtuales) no son parte de 802.1D, sino de IEEE 802.1Q.

2.2.9.7. Tipos De Puertos

Las VLAN utilizan puertos no seriales, es decir únicamente Ethernet: Ethernet, FastEthernet, Gigabit Ethernet.

2.2.9.8. Enlaces Troncales VLAN

Una troncal es una conexión física y lógica entre dos switches, entre un switch y un router, o entre un switch y un servidor (con una NIC especial que soporte *trunking*), a través del cual el tráfico de red viaja. Generalmente es un enlace punto a punto de 100 o 1000 Mbps. Es decir los puertos FastEthernet de un switch son configurable porque pueden funcionar para enlaces de acceso o enlaces troncales.

El propósito de las troncales es evitar poner un enlace por cada VLAN. Esta es una simple forma de implementar la comunicación de VLan's entre switches, pero esta no es escalable. Es importante entender que un enlace troncal no pertenece a ninguna VLAN específica. Simplemente es un conducto para VLAN's entre switches y routers.

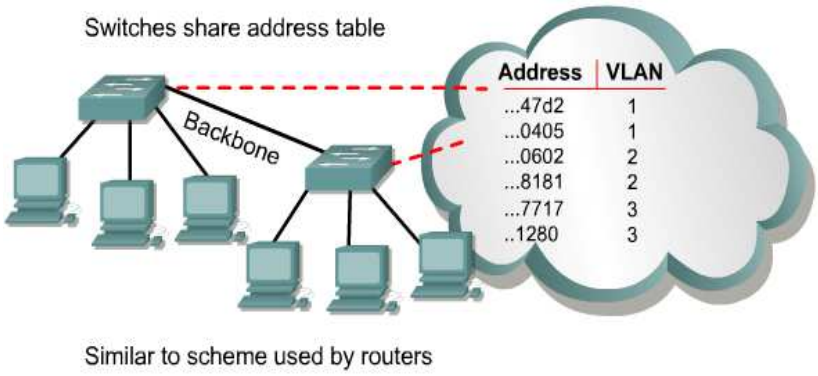
Las troncales permiten convertir a un simple puerto, en parte de múltiples VLANs al mismo tiempo. Lo cual es una verdadera ventaja, por ejemplo, actualmente se puede configurar para tener un servidor en varios dominios de broadcast simultáneamente, lo que quiere decir que usuarios de diferentes dominios de broadcast no necesitarán cruzar un dispositivo de capa 3 (router) para acceder al mismo servidor.

a) **Trunking con filtrado de tramas**

Las tablas de filtrado son creadas por cada switch, asociando cada dirección física con la VLAN a la que pertenece. Los switches comparten estas tablas a través del backbone. Por lo tanto, cuando llega una

trama a un switch, las tablas de conmutación en los dos extremos de la troncal son usadas para realizar las decisiones de envío basadas en las direcciones MAC de destino de las tramas.

Figura Nº 11: Filtrado de Tramas



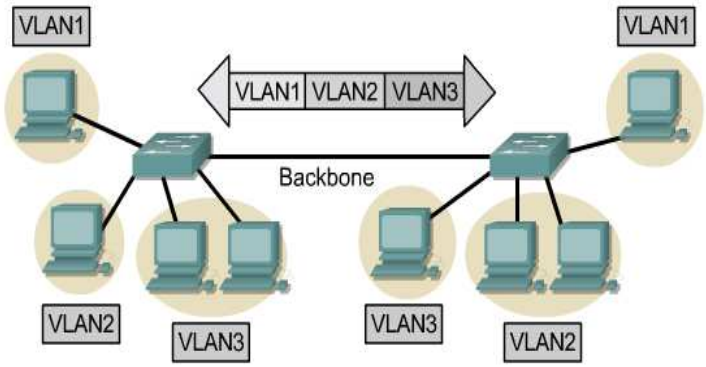
Fuente: http://www.cisco.com/web/learning/netacad

b) **Trunking con etiquetado de tramas**

Este método tiene asociado un identificador para cada VLAN, algunas personas se refieren a esto como el "VLAN ID" o "color". Las tramas procedentes de los usuarios, antes de ser enviadas a través del enlace troncal o backbone, se etiquetan con el identificador correspondiente a la VLAN a la que pertenecen.

Este identificador es entendido y examinado por cada switch antes de cualquier broadcast o transmisión a otros switches, routers o estaciones de trabajo. Una vez que la trama va a abandonar el backbone, entonces el switch elimina el identificador antes de ser enviada a la estación final.

Figura Nº 12: Etiquetado de Tramas



Fuente: http://www.cisco.com/web/learning/netacad

Los protocolos de trunking que usan etiquetamiento, consiguen la entrega de tramas en forma más rápida y hacen su manejo más fácil.

2.2.9.9. VLAN Trunking Protocol –VTP

VTP fue creado por Cisco para resolver problemas operacionales en una red conmutada con VLan's. Los dos problemas más comunes son:

- El cruce de VLan's causado por inconsistencias de configuración de VLANs.
- Falta de configuración de VLan's a través de medios mezclados como Ethernet y FDDI.

Es decir, el administrador de la red con la implementación de VTP evita configurar por separado cada switch, una tarea que requiere tiempo y adiciona costos operativos, dependiendo del tamaño de la red. A su vez, incrementa la posibilidad de errores o problemas de configuración.

El objetivo de VTP es mantener consistencia en la configuración de VLANs a través de un dominio de administración de red común. VTP es un protocolo de mensajes que usa las tramas de las troncales de capa 2 para añadir, eliminar y renombrar VLANs, información que luego es transmitida a todos los otros switches en el dominio del VTP. Un switch solo puede pertenecer a un solo dominio VTP.

a) **Beneficios de VTP**

- Consistencia en la configuración de la VLAN a través de la red.
- Seguimiento y monitoreo preciso de las VLAN.
- Informes dinámicos sobre las VLAN que se agregan a una red.
- Configuración de enlace troncal dinámico cuando las VLAN se agregan.

b) Funcionamiento VTP

- El VTP permite a un administrador de red configurar un switch de modo que propagaría las configuraciones de la

VLAN hacia los otros switches en la red.

- El switch se puede configurar en la función de servidor del VTP o de cliente del VTP.
- EL VTP solo aprende sobre las VLAN de rango normal.
- Tanto el servidor como el cliente intercambian las publicaciones entre ellos para asegurarse de que cada uno tiene preciso de la información de la VLAN.
- Las publicaciones del VTP no se intercambian si el enlace troncal entre los Switch es esta inactivo. Operación de VTP.

c) Componentes VTP

Dominio de VTP: Consiste de uno o más switches interconectados. Todos los switches en un dominio comparten los detalles de configuración de la VLAN usando las publicaciones del VTP.

Servidor del VTP: El servidor VTP publica la información VLAN del dominio del VTP a otros switches habilitados por el VTP en el mismo dominio del VTP. Los servidores VTP guardan la información de la VLAN para el dominio completo en la NVRAM. En el servidor es donde las VLAN se pueden crear, eliminar o modificar para el dominio.

Cliente del VTP: Funcionan de la misma manera que los servidores del VTP pero no pueden crear, cambiar o eliminar las VLAN en un cliente del VTP. Un cliente del VTP solo guarda información de la VLAN para el dominio completo mientras el switch está activado. Pero al realizar un reinicio del switch borra la información de la VLAN.

2.2.10. Listas de control de acceso - ACL

Las listas de control de acceso (ACL / Access Control List) incluyen una de descripción de los usuarios y grupos de usuarios con diferentes permisos sobre los archivos y carpetas de un volumen NTFS (New Technology File System).

Aparecer en la lista ACL significa tener derecho de acceso sobre el archivo o carpeta. El tipo de permiso definido en la entrada de un usuario o grupo de usuarios especifica el nivel de privilegio sobre el objeto (lectura, escritura, etc.).

Cada vez que un usuario accede a un archivo o carpeta se verifica si el usuario o el grupo de usuarios al que pertenece tienen al menos una entrada en la lista ACL del objeto. De no

ser así, el sistema le niega el derecho sobre el objeto; en cambio, si posee uno o más entradas, el usuario podrá acceder al objeto con los privilegios especificados por los permisos asociados a las entradas.

2.2.11. Definición de Calidad de Servicio (QoS)

QoS hace referencia a la capacidad de una red para proporcionar diferentes niveles de servicio al tráfico de red en diversas tecnologías. Los objetivos principales de QoS es el ancho de banda dedicado, controlar el jitter y la latencia (requerido por algunos servicios en tiempo real y el tráfico interactivo) y la pérdida de características mejoradas.

Las técnicas de trabajo en la congestión de una red, se utilizan para administrar y priorizar el tráfico en una Lan donde las aplicaciones solicitan más ancho de banda y que la red no es capaz de proporcionar. Al dar prioridad a ciertas clases de tráfico, estas técnicas permiten a las empresas retrasar las aplicaciones sensibles para que funcionen correctamente en una red congestionada.

QoS se puede dividir en tres niveles diferentes. Estos modelos de servicio se pueden describir en un conjunto de capacidades QoS de extremo a extremo.

QoS extremo a extremo, es la habilidad de la red para proporcionar un nivel específico de servicio de tráfico de un extremo a otro de la red. Los tres niveles de servicio son: El de mejor esfuerzo de servicio, servicio integrado y servicio diferenciado.

Mejor esfuerzo de servicio, como su nombre lo indica, es cuando la red hará todo lo posible para entregar el paquete del servicio a su destino. Con el mejor esfuerzo no hay garantías de que el paquete alcance su rumbo.

Modelo de servicio integrado, permite a las aplicaciones tener un nivel de servicio garantizado mediante la negociación de parámetros de red de extremo a extremo. Las aplicaciones pueden solicitar un nivel de servicio necesario para que funcionen correctamente y confiar en el mecanismo de calidad de servicio para reservar los recursos de red necesarios antes de que se inicie la transmisión de los paquetes de la aplicación. Es importante señalar que la aplicación no envía algún tipo de tráfico hasta que reciba una señal de la red la cual le indica que la red puede manejar la carga y entregar a

su destino un QoS.

Modelo de servicios diferenciados. El cual incluye un conjunto de herramientas de clasificación y gestión de colas para la prestación de algunos protocolos o aplicaciones con una cierta prioridad sobre el tráfico de la red. Los servicios diferenciados se basan en los routers de extremo para realizar la clasificación de los diferentes tipos de paquetes que pasan por una red.

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y videovigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de manera distinta para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

El término Calidad de Servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación. El tráfico PTZ, que a menudo se considera crítico y requiere una latencia baja, es un caso típico en el que la QoS puede garantizar respuestas rápidas a solicitudes de movimiento

Figura 2.18 Tabla de Priorización de QoS.

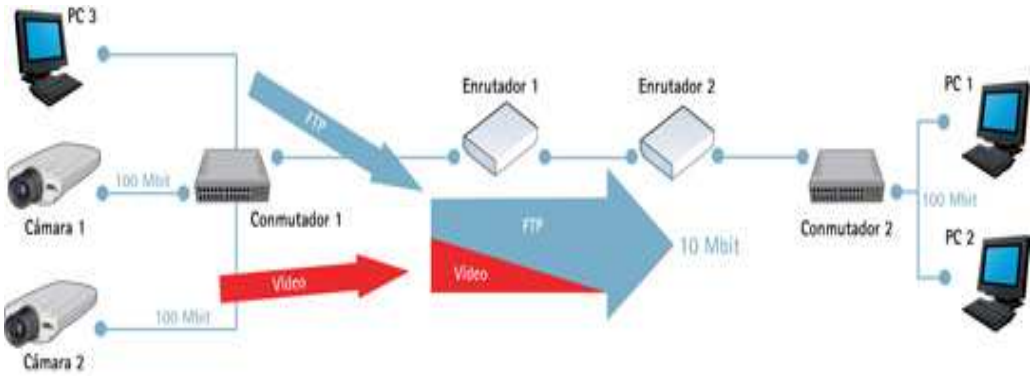
CoS	Prioridad	Descripción de las clases de servicios
Voz	Real Time	Tráfico Multimedia: Voz sobre IP
Video	Video	Tráfico Video : Video conferencia, vídeo sobre demanda, vídeo "broadcast"
Datos	Platina	Tráfico Datos Alta Prioridad: SNA, SAP, Aplicaciones muy críticas
	Oro	Tráfico Datos Media Prioridad: Aplicaciones críticas, LAN to LAN, e-mail
	Plata	Tráfico de Datos baja prioridad: Intranet
	Bronce	Tráfico de Datos Best Effort: Internet

Fuente: http://en.wikipedia.org/wiki/

Red sin QoS En este ejemplo, PC1 está reproduciendo dos secuencias de vídeo de las cámaras 1 y 2. Cada cámara transmite a 2,5 Mbit/s. De repente, PC2 inicia una transferencia de archivos desde PC3.

En este escenario, la transferencia de archivos intentará utilizar la capacidad total de 10 Mbit/s entre los enrutadores 1 y 2, mientras que las secuencias de vídeo intentarán mantener su total de 5 Mbit/s. Así, ya no se puede garantizar la cantidad de ancho de banda destinada al sistema de vigilancia y probablemente se reducirá la frecuencia de imagen de vídeo. En el peor de los casos, el tráfico del FTP consumirá todo el ancho de banda disponible. Ver Figura 14

Figura Nº 14: Gráfica sin aplicación de QoS

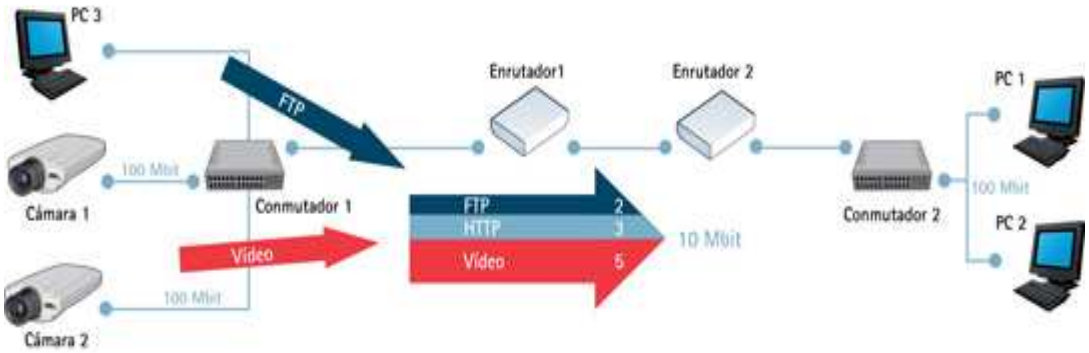


Fuente: http://www.axis.com

Red con QoS. En este escenario, se ha configurado el enrutador 1 para dedicar hasta 5 Mbit/s de los 10 disponibles a la transmisión de vídeo. El tráfico del FTP puede utilizar un máximo de 2 Mbit/s, y HTTP, junto con el resto del tráfico, pueden utilizar un máximo de 3Mbit/s. Con esta división, las transmisiones de vídeo siempre tendrán disponible el ancho de banda que necesitan.

Las transferencias de archivos se consideran menos importantes y, por lo tanto, obtienen menor ancho de banda; sin embargo, aún quedará ancho de banda disponible para la navegación web y el resto del tráfico. Hay que tener en cuenta que estos valores máximos sólo se aplican en caso de congestión en la red. El ancho de banda disponible que no se use se podrá utilizar por cualquier tipo de tráfico.

Figura Nº 15: Gráfica con aplicación de QoS



Fuente: http://www.axis.com

No es fácil encontrar una definición para la calidad de servicio. Cada servicio tiene su propia definición para QoS y cada servicio puede ser descrito por sus características QoS. Para el desempeño de una red de comunicación de datos, las características QoS son: ancho de banda, retardo y confiabilidad.

2.2.12. Tecnología ADSL

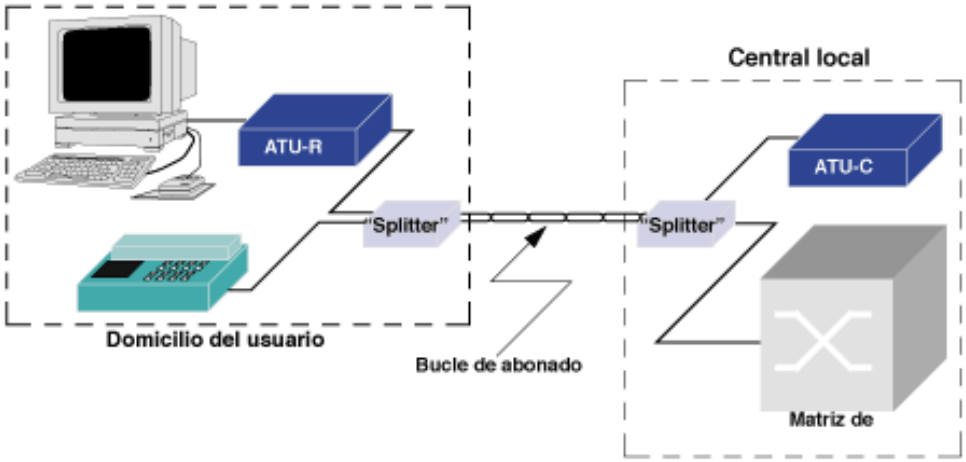
El ADSL es una tecnología de banda ancha que permite que el ordenador reciba datos a una velocidad elevada, todo ello a través de la línea de teléfono convencional mediante la modulación de la señal de datos utilizada por el ordenador.
Una de las características del ADSL, que ha contribuido a la utilización de esta tecnología al uso de Internet ha sido que se trata de un sistema asimétrico, en el cual la velocidad de transmisión en ambos sentidos no es el mismo. En una conexión a Internet normalmente la velocidad de transmisión de bajada (Internet - Host) suele ser mayor que la de subida (Host - Internet). Un ejemplo de ello está en un acceso a una página Web, para realizarlo debemos hacer una petición al servidor correspondiente de que queremos acceder a la pagina en cuestión, todo ello se realiza con una transmisión de unos pocos Bytes, mientras que el servidor a nosotros nos manda la página entera que puede ocupar unos Kbytes has varios Mbytes, con lo que vemos que es necesario una mayor velocidad de bajada.

Funcionamiento del ADSL

El ADSL es una técnica de modulación de la señal que permite una transmisión de datos a gran velocidad a través de un par de hilos de cobre (conexión telefónica).
La primera diferencia entre la modulación de los módems de 56K y los de ADSL es que esto modulan a un rango de frecuencias superior a los normales [24... 1.104] KHz para los

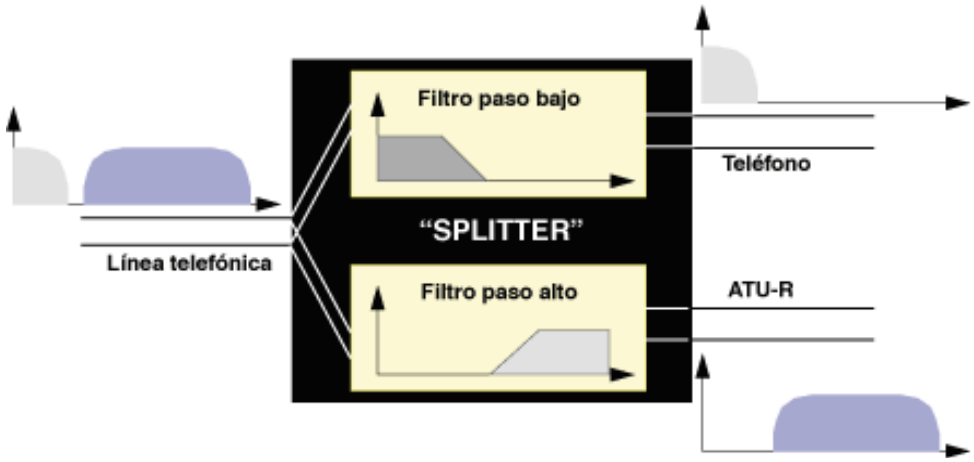
ADSL y [300... 3.400] Hz para los normales la misma que la modulación de voz, esto supone que ambos tipos de modulación pueden estar activos en un mismo instante ya que trabajan en rangos de frecuencia distintos.
La conexión ADSL es una conexión asimétrica, con lo que los módems situados en la central y en casa del usuario son diferentes. Vemos que los módems son diferentes y que además entre ambos aparece un elemento llamado 'splitter', este está formado por dos filtro uno paso alto y otro paso bajo, cuya única función es separar las dos señales que van por la línea de transmisión, la de telefonía vocal (bajas frecuencias) y la de datos (altas frecuencias).

Figura Nº 16: Conexión ADSL



Fuente: http://www.adslzone.net/

Figura Nº 17: Funcionamiento del Splitter.

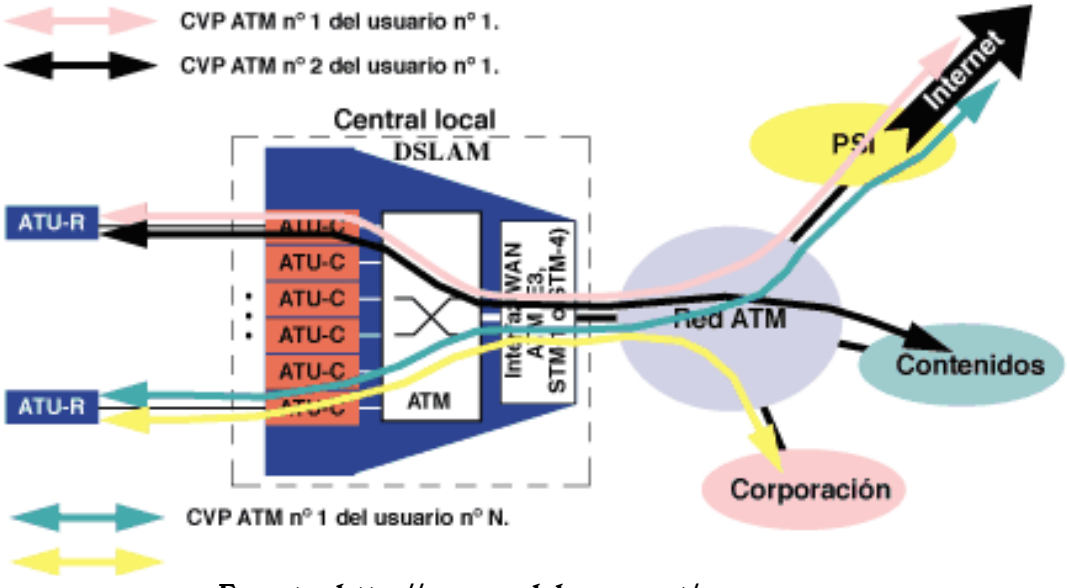


Fuente: http://www.adslzone.net/

2.2.13. ATM sobre ADSL

Las ventajas del ADSL son el gran ancho de banda en el acceso, dicho ancho de banda se encuentra activo de forma permanente y finalmente aprovecha la infraestructura desplegada para el sistema telefónico.
Para obtener el máximo rendimiento que esta tecnología nos proporciona, las redes de comunicación de banda ancha utilizan el ATM ('Asychronuos Transfer Mode') para la comunicación. Desde el principio ADSL se concibió para el envío de información a gran velocidad, se pensó en el envío de dicha información en celdas ATM sobre los enlaces ADSL. Esto tiene una sencilla explicación, puesto que si usamos en un enlace ADSL el ATM como protocolo de enlace podemos definir varios canales virtuales permanentes (PVC), cada uno dedicado a un servicio diferente. Esto aumenta la potencia de esta tecnología, pues añade flexibilidad para múltiples servicios a un gran ancho de banda.
Finalmente otra ventaja añadida es que en ATM se contemplan diferentes velocidades de transferencia con distintos parámetros para la calidad del servicio, así podemos dar un tratamiento diferente a cada una de estas conexiones, lo que a su vez permite dedicar el circuito más adecuado por sus parámetros de calidad de servicio a cada tipo de aplicación, ya sea voz, video o datos.

Figura N° 18: ATM. Sobre ADSL.



Fuente: http://www.adslzone.net/

En los módems ADSL se pueden definir dos canales:

- 'Fast': Utilizado para comunicaciones por voz, más sensibles al retardo.
- 'Interleaved': Utilizado para aplicaciones sensibles a la perdida de información.

2.2.14. Evolución de la red de acceso

Los nuevos estándares del ADSL han conseguido unas velocidades de transferencia espectaculares, teniendo en cuenta el medio físico por el que circulan. En concreto los módems son capaces de transmitir a 8,192Mbps en sentido descendente y 0,928 Mbps en sentido ascendente.
Con estas cifras el despliegue de esta tecnología supone una autentica revolución en la red de acceso de la operadoras del servicio telefónico dichas líneas pasan de ser de banda estrecha capaces de transmitir voz o datos con módems de bajas velocidades, a ser redes de banda ancha multiservicio.
La red de acceso deja de ser el gran obstáculo que tenían las operadoras para el desarrollo y oferta de nuevos servicios, inimaginables hasta hace pocos años.

2.2.15. Herramientas de Simulación - Redes

- **Simulación**

  La simulación es la imitación del funcionamiento de un sistema real durante un intervalo de tiempo. Esta simulación puede realizarse ya sea de forma manual o en forma computacional.

  Actualmente las herramientas de simulación son de gran utilidad debido a que se puede prever el comportamiento de un sistema antes de implementarlo, se pueden encontrar comportamientos del sistema que no se detectan fácilmente por la complejidad del estudio y una razón muy importante en cualquier empresa es el ahorro de dinero porque ayuda al diseño y perfeccionamiento del sistema a construir.

  Existen muchos software de simulación, los que no necesitan que se realice un análisis del sistema para desarrollar el sistema, sino que solo se requieren datos de entrada para su uso, los cuales también brindan facilidades de uso y de análisis de los resultados entregados.

Cuadro Comparativo – Herramientas de Simulación Lan

Software	Valor Descriptivo
Network Simulator Tesbed	Este software brinda un ambiente de simulación para sistemas de redes distribuidas y protocolos básicos. Utiliza una interfaz gráfica que permite controlar la simulación. Está basado en una arquitectura cliente/servidor, lo que permite que complejos escenarios de simulación sean ejecutados en servidores remotos con mayores capacidades de cálculo. Fue implementado en C y permite a los usuarios ejecutar sus propios códigos escritos en este mismo lenguaje.
Maryland Routing Simulator	Es otro Simulador de eventos discretos, este programa es un desarrollo evolutivo de un simulador más antiguo llamado NetSim. Está desarrollado en lenguaje C en una plataforma Unix, posee dos interfaces gráficas (Xlib y Motif) y una en modo texto. Enfocado al estudio de algoritmos de ruta en redes WAN.
Network Simulator 2 (ns-2)	Este software surge a partir de REAL network simulator. Incorporando funcionalidades de Routing y multicast en redes estructuradas y wireless. Fue implementada en C++, pero para realizar las simulaciones usa un lenguaje interpretado llamado Tcl. Además cuenta con un visualizador llamado Nam, que permite ver en forma más cómoda los resultados de la simulación.
NCTUns 2.0 Network Simulator/Emulator	Esta herramienta para realizar las simulaciones usa el mismo protocolo TCP/IP que se encuentre en el computador donde se ejecuta el programa, dando un mayor desempeño a la simulación. Entre los tipos de redes que puede simular se cuentan redes estructuradas con host fijos, LAN wireless, redes OBS, entre otros. Entre los dispositivos de red se pueden contar hubs ethernet, switches, router, host, estaciones y puntos de acceso wireless IEEE 802.11(b), estaciones base GPRS, switches ópticos, etc.
Packet Tracer Cisco	Es una utilidad software para crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Se enfoca en apoyar mejor los protocolos de red. Hoy en día es la herramienta de simulación más utilizada, conforme los productos de la Familia Cisco van ganando terreno en el mercado de equipos orientados al soporte de la Plataforma de Red. **Soporta los siguientes protocolos:**

	• HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS. • TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6. • RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas. • Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP, ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

2.2.16. Cuadro comparativo de Instrumentos de Medición LAN

Software	Valor Descriptivo
CommTraffic	Es una utilidad de red para coleccionar, procesar y mostrar tráfico y estadísticas del uso de una red para conexiones LAN y dial-up. En un segmento de LAN, muestra estadísticas del tráfico y uso de red para cada ordenador. Es una aplicación personalizable, que muestra estadísticas gráficas y numéricas. Permite generar una serie de reportes que reflejan el volumen de tráfico de la red, el gasto de conexión a Internet, ver estadísticas para hosts local y remoto, protocolos IP y puertos TCP/UDP remoto/local.
CommView	Es un software diseñado para mostrar el trafico de red mediante cuadros estadísticos, sin embargo su mejor versión como instrumento de medición radica en la versión *CommView for WiFi* que es una edición del programa CommView diseñada para capturar y analizar paquetes en redes wireless 802.11a/b/g. Recoge información desde adaptadores wireless y decodifica los datos analizados.
AirPort Flow	Es una pequeña utilidad que nos permite monitorizar el tráfico de red, permitiendo básicamente ver el tráfico TCP que entra y sale del router. Posee dos gráficas muy sencillas que nos muestran el tráfico que entra y sale, con indicaciones acerca de los picos de tráfico. Desde su panel de preferencia se puede configurar la dirección IP del router, el valor IF y contraseña si se tiene.
NTOP (Network TOP)	Utilidad software para monitorear y medir en tiempo real el tráfico por usuario y aplicaciones que están consumiendo recursos de red, detecta malas configuraciones, analiza datos de flujos de la industria enviados por los routers. Es un software considerado como administrador del tráfico de red. Está escrito en lenguaje Perl, funciona en sistemas Unix, Linux, Windows y Netware. Crea los logs tomando una muestra de cualquier contador snmp y lo grafica en paginas html integrando una lista de gráficos que representan los datos obtenidos de cada dispositivo.

MRTG (Multi Router Traffic Grapher)	Funciona bajo el protocolo SNMP (simple network management protocol). Es un software también considerado como administrador del tráfico de red. Está escrito en lenguaje Perl, funciona en sistemas Unix, Linux, Windows y Netware. Crea los logs. A nivel de rendimiento se asemeja mucho al aplicativo NTOP, considerando su capacidad de procesamiento y muestreo del estado de la Lan, es también considerada uno de los mejores aplicativos.

2.2.17. Tecnologías de Seguridad Emergentes

Windows Server 2008 – NAP (NetWork Access Protection)

En la actualidad las redes corporativas y las no corporativas son cada día más complicadas de administrar y securizar. Los escenarios presentan cada vez circunstancias de mayor dificultad en cuanto a conectividad y seguridad Lan, por lo cual las múltiples amenazas de seguridad posibles como pueden ser **malware, exploits, spyware, DOS, Script-Kiddies y otros.** Estas aplicaciones pueden tomar el control del sistema, realizando acciones dañinas de forma totalmente transparente, llegando a comprometer el sistema como puerta de entrada de otras amenazas.
La característica NAP (NetWork Access Protection) es una de las novedades que ofrece **Windows Server 2008** en cuanto a **Herramientas de Seguridad en Lan's.** Con NAP podemos aplacar el impacto de situaciones como las antes indicadas, y optimizar el nivel de protección de la red corporativa y la información contenida en la misma. Por ello este nuevo aplicativo se presenta como alternativa de seguridad de alto nivel dentro de las gamas de tecnologías emergentes.

Características:

- Plataforma que fuerza el cumplimiento de unos estados de salud para el acceso a Redes.
- Establece redes de cuarentena a la espera de cumplir los diferentes criterios.
- Componentes de Sistema Operativo: Servidor NAP – Windows Server 2008 / Cliente NAP – Windows Vista, Windows XP SP2, Windows Seven.
- Permite la integración con Sistemas de terceros.

Componentes de NetWork Access Protection:

- Métodos para forzar el cumplimiento Network Access Protection.

    - Validar el estado de salud.
    - Aplicación de remedios.
    - Limitar el acceso.
  - Network Policy Server (NPS)
    - Sustituye a Servicios de Autentificación de Internet Service (IAS) de Windows Server 2003.
    - Servidor de políticas para Network Access Protection.
  - Componentes de infraestructura.
    - Switch.
    - DHCP.
    - Terminal Server, etc.
  - Servicio de Directorio Activo.
    - Almacena las cuentas de usuario y equipo que serán utilizados para autentificar las conexiones.
  - Servidor de salud de Certificados.
    - Ofrece certificados para equipos que contemplen las condiciones de salud.
  - Servidores de Remedio.
    - Utilizado por SHAs (System Health Agent) donde el estado de salud de un equipo es monitorizado por una parte del cliente NAP.
- Servidor de Políticas.
  - Utilizado por SHV (System Health Validators) para analizar el estado de salud de los clientes NAP. Incorpora políticas de red, y determina la acción a tomar basándose en el estado de salud del equipo que se conecta.

Validación de la Política de Salud en NAP

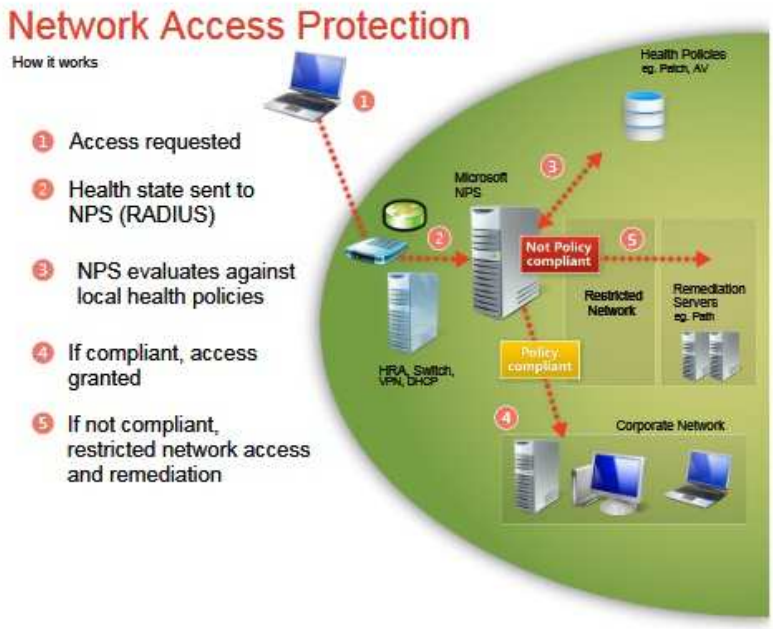
- Los equipos parametrizan las condiciones exigidas por el Servidor NPS.
- Equipos que cumplen.
  - Ganan acceso ilimitado.
  - Equipos que no cumplen las condiciones o no son compatibles con NAP : Tienen acceso ilimitado pero se registra un log de estado.

- Acceso limitado a redes restringidas.

Hay equipos que pueden estar exceptuados del cumplimiento NAP. **Aplicación de Remedio en NetWork Access Protection**

- Aquellos equipos que no cumplan con las condiciones de seguridad, pueden aplicarse métodos automatizados para remediarlo.
  - Levantar servicios automáticamente.
  - Ejecutar procedimientos.
  - Iniciar los procedimientos de actualización de Sistema Operativo o soluciones de seguridad.
  - Notificaciones.

Figura Nº 19: Dinámica de NAP



Fuente: http://www.microsoft.com/windowsserver2008/en/us/nap-details.aspx

Si a todo esto añadimos un servidor WSUS, el cliente NAP puede verificar que las últimas actualizaciones de seguridad están instaladas en el equipo, basándose en uno de los cuatro niveles de seguridad establecidos por la plataforma Microsoft Security Response Center (MSRT).

Un ejemplo de posible intervención de esta tecnología seria en una política de seguridad donde los equipos deban disponer del Firewall Windows activado, si habilitamos la opción en automático (servicios de remediación), aquel cliente que no tenga disponga del firewall de Windows activado, sería enviado a un segmento de red de cuarentena, y los componentes NAP del cliente habilitarían el firewall de Windows sin intervención del usuario.

Operativa de NetWork Access Protection en diversos escenarios.

- Tráfico protegido con IPSEC.
- 802.1X.
- VPN con acceso remoto.
- DHCP IPV4 (tanto para renovación como concesión de direcciones).

• **NAP para entornos IPSEC.** Para la implementación de NAP en entornos con IPSEC es necesario implantar una entidad certificadora de salud (HRA Server), un NPS Server y un cliente IPSEC. El HRA publica los certificados de salud X.509 para los clientes NAP. Estos certificados son utilizados para autenticar los clientes NAP cuando éstos inician una comunicación basada en IPSEC con otros clientes NAP de la intranet. Este es el método más seguro de aplicar NAP.

• **NAP para entornos 802.1X.** Para implementar esta solución, necesitamos desplegar un servidor NPS y un componente (EAP). El servidor NPS envía la autenticación basada en 802.1X a un punto de acceso de la red interna. Si el equipo cliente no cumpliese con alguna regla establecida, el servidor NPS limitaría el acceso al cliente mandando al punto de acceso un filtro basado en dirección IP o identificador virtual.

• **NAP para entornos VPN (Virtual Private Network).** En esta ocasión necesitamos de un servidor y un cliente VPN. Usando NAP para entornos VPN, los servidores VPN pueden forzar el cumplimiento de la política de salud de la empresa cuando los clientes externos se conecten a nuestra intranet. Esta solución proporciona los mecanismos necesarios para establecer una comunicación segura entre un cliente externo y la red interna.

• ***NAP para entornos de configuración dinámica de direcciones (DHCP).*** Para implementar esta solución, necesitamos el componente NAP de un servidor DHCP y un servidor NAP. Usando DHCP, podemos cumplir con la política de salud de la empresa a través de NPS y DHCP cuando un equipo intente renovar o solicitar una dirección IP (IPV4). El servidor limitaría el acceso a los equipos que no cumpliesen con la política de salud de la empresa asignando direcciones IP reservadas para tal fin.

Cada uno de estos métodos de implementación NAP tiene sus ventajas e inconvenientes, por lo que implantar una plataforma de este tipo en una corporación dependerá en gran medida de las necesidades de servicio y condiciones operativas de ésta. NAP adicionalmente proporciona una API para desarrolladores que necesiten integrar su software a las necesidades de la empresa. Con

ello las posibilidades de personalización de las soluciones es aún mucho mayor.

Windows Server 2008 – File Screening Management

File Screening Management o Bloqueo de Archivos, viene dentro de la tecnología de File Server Resource Manager (El Gestor de Recursos del Servidor de Archivos). Con esta característica podemos evitar que los usuarios ya no guarden en los servidores de archivos los populares archivos de música, videos o cualquier otro tipo no permitido.
Las excepciones a estas parametrizaciones pueden ser creadas o configuradas para ser admitidas a determinados usuarios. Con ello esta herramienta se presenta como una alternativa para reforzar el tema de la seguridad y mejor administración de la data en espacios de disco en los servidores corporativos.
File Screening Management permite establecer límites de espacio de almacenamiento en volúmenes y carpetas, evitar que los usuarios puedan guardar ciertos tipos de archivos en el servidor y generar una serie de informes de almacenamiento muy completos.
Con todo ello no solo ayuda a gestionar y monitorizar los recursos de almacenamiento actuales desde un lugar central, sino que facilita la planificación e implementación de cambios dentro de la infraestructura de almacenamiento.

2.2.18. SNMP (Simple Network Management Protocol)

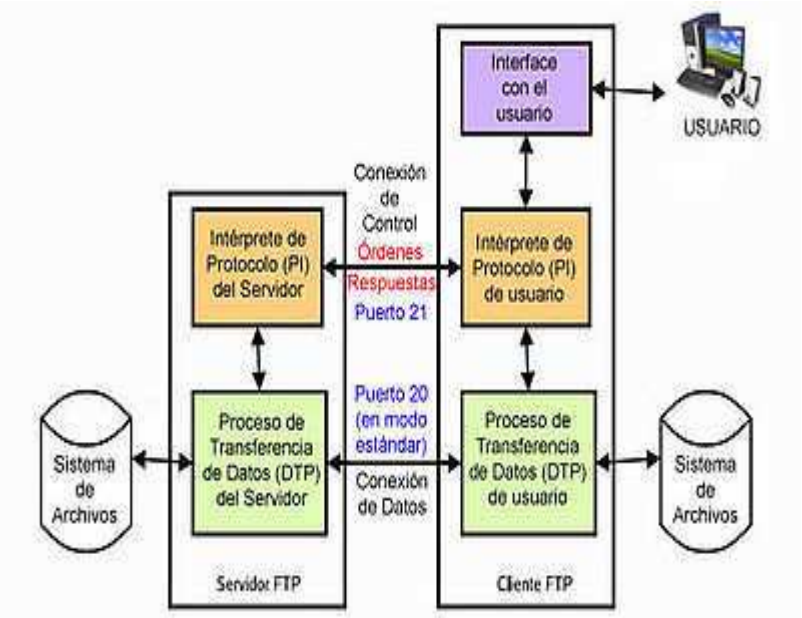
El Protocolo Simple de Administración de Redes –SNMP- (Simple Network Management Protocol), es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre los dispositivos de red, pertenece al conjunto de protocolos de TCP/IP. SNMP permite a los administradores de red administrar el rendimiento de la red, encontrar y resolver problemas de red y planificar el crecimiento de la red.
Existen dos versiones de SNMP: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen características en común, pero SNMPv2 ofrece mejoras con operaciones adicionales.

2.2.19. FTP (File Transfer Protocol)

FTP (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar enviar archivos,

independientemente del sistema operativo utilizado en cada equipo.
El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos.
Para solucionar este problema son de gran utilidad aplicaciones como Scp y Sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

Figura. Nº 20: Diagrama Servicio FTP.



Fuente: http://es.wikipedia.org/wiki/File_Transfer_Protocol

a) Servidor FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.
Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación

FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

b) Cliente FTP

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesitará utilizar un programa cliente FTP.
Un cliente FTP es un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos.
Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

c) Ventajas de los FTP.

- Los programas FTP permiten reanudar las descargas interrumpidas por cortes de conexión o cualquier otra circunstancia en el mismo punto donde se quedaron.
- Son tan fáciles de usar como el Explorador de Windows: no hay que utilizar complicados comandos ni teclear orden alguna. Para descargar un archivo, basta con arrastrarlo con el mouse desde una ventana (el servidor remoto) a otra (el disco duro)
- Permiten hacer descargas masivas y automatizadas en segundo plano, mientras se realizan otras tareas con el computador; así el usuario puede despreocuparse de la descarga hasta que finaliza.
- También facilitan la transferencia de archivos de un servidor remoto a otro. En la mayoría de los casos, estas transferencias son mucho más rápidas que cuando se realizan a través de la conexión personal.

2.2.20. LACP (Link Agreggation Control Protocol)

El Protocolo de Agregación de Enlaces de Control – LACP, es un protocolo definido en el estándar 802.1ad y que puede ser implementado en los switches. LACP permite agrupar puertos por su velocidad, modo dúplex, trocales, VLAN, sumando la velocidad nominal de cada puerto físico y así obtener un único enlace troncal de alta velocidad.

La ventaja principal de LACP es que posee el ancho de banda de red de todos sus adaptadores en una sola presencia en la red. Si un adaptador tiene una anomalía, el tráfico de la red se envía al siguiente adaptador disponible de forma automática, sin interrumpir las conexiones del usuario existentes. El adaptador se devuelve automáticamente al servicio de Agregación de enlaces cuando se recupera y esto nos proporciona:

- ✓ Alta disponibilidad (si unimos 3 enlaces y cae uno de ellos, el enlace "lógico" seguirá siendo operativo)
- ✓ Balanceo de carga (en base al algoritmo de balanceo elegido, los datos se repartirán entre los enlaces reales)
- ✓ Mayor ancho de banda (matizable)
- ✓ Tiempos de convergencia reducidos en caso de fallo de algún link (STP)

Las conexiones LACP pueden interconectar switches, routers, servidores y clientes, su implementación es recomendable en enlaces sobre puertos de acceso, uno por VLAN.

III. MATERIALES Y MÉTODOS

3.1. Tipo de estudio y diseño de contrastación de hipótesis

La investigación por su naturaleza es Aplicada y con un diseño cuasi experimental porque no va a haber manipulación de variables independientes y éstas se miden o recolectan a través del tiempo en puntos o períodos especificados para hacer inferencias respecto al cambio en las variables dependientes.

Para el diseño de la contrastación de la hipótesis se utiliza el Método de Diseño con un grupo único con medición Antes y Después, que consiste en:

- Una medición previa de la variable dependiente a ser utilizada antes de la aplicación de la variable independiente.
- La aplicación de la variable dependiente o estímulo.
- Una nueva medición de la variable dependiente después de la aplicación de la variable independiente.

Se tomará el/los actor(es) involucrados en los Procesos soportados en la Red de Datos para realizar las actividades de sus procesos tal y como son llevados a cabo, sin el diseño propuesto, y se tomará una medición de los indicadores definidos. Luego de esto se simulará el nuevo diseño, para que haciendo uso de éste se determine los valores para los indicadores.

Finalmente se tomarán los datos obtenidos como resultado del proceso actual y del proceso con el nuevo diseño para verificar que sean exactos y se evaluará si realmente hubo o no una reducción considerable en el tiempo de procesamiento de los datos.

Para esto se toman medidas en dos instancias diferentes:

La Primera, se realizará al iniciar el proyecto, para reflejar los valores de los indicadores definidos

Segunda Instancia, realizar con la Prueba de Campo, que examinará los indicadores del rendimiento de la Red simulada por el proyecto.

3.2. Población, Muestra De Estudio Y Muestreo

La población a investigar para este proyecto está conformado por los 65 usuarios con acceso a la Red LAN de la empresa Editora El Comercio - Planta Norte, considerando que ellos son los principales afectados, puesto que siempre están supeditados a estas dificultades de la interconexión entre las áreas de la empresa y las oficinas descentralizadas de la Planta norte ubicadas en las ciudades de Piura, Chiclayo, Trujillo y Chimbote.

3.2.1. Muestra.

El tamaño de la muestra se obtiene aplicando la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + (Z^2 * P * Q)}$$

Donde:

0 N = Universo
1 e = 0.05 (Máximo de error permisible)
2 Z = 1.96 (Valor tabla) (95%)
3 P = 0.5 (Proporción de la población)
4 Q = 0.5 (1-P)

Para nuestro estudio tenemos:

$$n = \frac{1.96^2 * 0.5 * 65}{(64) * 0.05^2 + (1.96^2 * 0.5 * 0.5)}$$

$$n = 28.43 = 49$$

La muestra a considerar para el estudio son 29 usuarios cuyas operaciones o actividades serán medidas dentro de intervalos de tiempo de menor y mayor saturación en la red, como son las horas pico (5:00 pm a 9:00 pm).

3.2.2. Muestreo

Para el muestreo se toman los usuarios que forman parte de la muestra y que pertenezcan a las áreas que en el momento de la medición presenten una mayor recarga de trabajo con los servicios de red, especialmente en las horas pico. Los parámetros para la obtención de la información estadística, serán obtenidos mediante herramientas de medición como NTOP y de trafico Tracer Plus Ethernet y con el paquete Wireshark, donde se considero su puesta en marcha en horarios de altas tasas de transferencias de información, archivos que "pesan" en promedio de 30 MB a 80 MB, cuyos resultados se utilizaran para su posterior análisis.

3.3. Métodos, Técnicas e instrumentos de recolección de datos.

3.3.1. Métodos

El método que se utiliza en la investigación, es el Científico dado que se ejecuta a partir de una situación problemática real, abordándose con la construcción teórica en que se fundamenta para la elaboración y verificación de la hipótesis.
Al mismo tiempo, se presenta la teoría, referente al problema. Se recolecta información de cada variable, explorando y

describiendo las características relevantes enfocadas al problema, así como la aplicación de tales ideas mediante la simulación del diseño de red.

3.3.2. Técnicas

Las técnicas para la recolección de datos que se utilizan en el estudio, son: La Observación, Encuesta, La Entrevista y Software de simulación y medición de indicadores de Red. La encuesta se define como un procedimiento que consiste en hacer las mismas preguntas, a una parte de la población, que previamente fue definida y determinada a través de procedimientos estadísticos de muestreo.
La Entrevista realiza un procedimiento similar a la encuesta con la diferencia que las preguntas se desarrollan de forma oral obteniendo las respuestas de igual forma.
Se utilizan éstas técnicas, porque permiten conocer información de determinados hechos a través de las opiniones de grupos o individuos en presencia del investigador responsable de recolectar la información; se pretendió recopilar datos válidos y confiables referentes a los problemas, efectos, y fortalezas estimulados en la administración y gestión de las redes de área local.
La entrevista fue aplicada a varios gerentes de la empresa; mientras que la encuesta a los usuarios de la red LAN de la empresa editora El Comercio Planta Norte y Oficinas Descentralizadas.
El Software que se usó para la obtención de los valores de indicadores de rendimiento de la Red LAN es NTOP (Network TOP) que es un software libre de análisis del tráfico de red y permite monitorizar en tiempo real, mediante la utilización del protocolo SNMP, los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto.

Lo que hace Ntop, es estar monitorizando toda la red en busca de datos para generar estadísticas. Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, ARP.

3.3.3. Instrumentos.

Se selecciona El Cuestionario y La Guía de Preguntas como instrumentos para la recolección de los datos. El cuestionario, contiene preguntas cerradas y categorizadas. Las razones que justifican dicha elección se derivan de las ventajas proporcionadas por este instrumento; haciéndose más fácil la posterior tabulación e interpretación de los resultados.

La guía de preguntas, consta de una serie de interrogantes dirigidas a la gerencia o dueños propietarios de las empresas, con el objeto de obtener información referente a la disponibilidad de adoptar o no, la tecnología inalámbrica aplicada a las redes de computadoras.

3.3.4. Procedimiento

El procedimiento se basa en el Método o Metodología para el Diseño de una Red LAN. Para seleccionar la metodología a usar se evaluaron entre 4 diferentes modelos, se tomaron algunos criterios a medir para cada uno de estos métodos.

3.4. Plan de procesamiento para análisis de datos

Los parámetros para la obtención de la información estadística, serán obtenidos mediante herramientas de medición como NTOP, donde se considero su puesta en marcha en horarios de altas tasas de transferencias de información, archivos que "pesan" en promedio de 9 MB a 30 MB, cuyos resultados se utilizaran para su posterior análisis.

Este procedimiento se utilizará para agrupar los datos por medio de computadoras, a tabular, ponderar e interpretar los datos usando una hoja de cálculo en Excel, serán presentados la información recopilada por medio de encuestas que serán transcritas a su posterior análisis, en este caso el indicador estadístico serán presentados como información en forma de cuadros y gráficos.

IV. RESULTADOS

4.1. Desarrollo de la metodología Cisco Systems

4.1.1. Fase 1:

A. Situación de la empresa

El diseño de la red LAN se basa en la estructura corporativa de la empresa, conformada por 11 áreas, las cuales se encuentran distribuidas en los siguientes departamentos:

- Departamento de Administración
- Departamento de Pre prensa
- Departamento de Redacción
- Departamento de Seguridad
- Departamento de Publicidad
- Departamento de Rotativa
- Departamento de Despacho
- Departamento de Circulación
- Departamento de Mantenimiento
- Departamento de Almacén
- Departamento de Sistemas

En esta etapa iniciamos el proceso de recopilación de información en la Empresa Editora El Comercio S.A. – Planta Norte, para así identificar los problemas de la red actual, apoyado también en parámetros como el crecimiento anual y proyecciones de crecimiento, procedimientos de administración, sistemas, redacción, publicidad y el resto de las áreas anteriormente mencionadas. Para ello, se planteó los siguientes puntos al reunir la información:

a) Personas que utilizan la red.
b) Operaciones que han sido declaradas críticas por la organización.
c) Equipos.
d) Hosts instalados.
e) Arquitectura de software.
f) Calidad de Servicio.
g) Recursos para brindar seguridad Lan.
h) Personas que utilizan la red

Están comprendidas dentro de las 11 áreas con las que cuenta actualmente la empresa, como son Administración, Redacción, Pre prensa, Seguridad, Publicidad, Rotativa, Despacho, Circulación, Mantenimiento, Almacén y Sistemas, que en conjunto agrupan a 65 trabajadores.

El personal involucrado dentro de la organización, requiere en los procesos individuales o grupales mayor Ancho de Banda en horas críticas (Entre 8 MB/s y 10 MB/s) y mejoras en los parámetros de seguridad de la red (Resultados de encuesta interna y análisis de vulnerabilidades LAN).

Para ello, la propuesta de implementar redes virtuales para segmentar la red y configurar nuevos estándares de seguridad en equipos de comunicación, parte de la premisa de elevar la eficiencia y efectividad de todos los trabajadores. Estas mejoras se plasman en la reducción de tiempos de procesos de alta prioridad, mejorar la flexibilidad, mediante Tolerancia a fallas y mayor escalabilidad, brindar mayores controles de seguridad para asegurar la integridad de la información; todo ello apoyado en una plataforma estratégicamente configurada.

B. Operaciones que han sido declaradas críticas por la organización.

Mediante un análisis de los distintos procesos productivos y administrativos que se llevan a cabo en la empresa, se clasificaron y puntualizaron de acuerdo al grado de impacto que poseen dentro de los procesos core del negocio.

C. Data:

- Si el "tamaño" de la información aumentara de manera exponencial, la red de datos actual se degradaría en horas pico en índices por debajo de lo aceptable (10 Mb/s a 8 Mb/s), generando un impacto en el tráfico de la red actual y afectando a todos los sistemas.

D. Equipos :

- Telefonía IP: Si los enlaces telefónicos fallasen permanentemente, originaría un retraso en los procesos periodísticos, control de calidad de páginas de los diarios y retraso en la coordinación interdepartamental y externa, para la toma de decisiones y procesos a seguir.
- Los switch Cisco Catalyst 3560 y Router Cisco 2800 Series, están configurados con funciones predeterminadas, donde no se está explotando al máximo el potencial de los equipos.

E. Seguridad:

- Este segmento conforma la columna vertebral de la plataforma Lan, donde si se ve vulnerada, el impacto podría afectar seriamente procesos, tareas, actividades, etc. Un ejemplo de ello es el compartir recursos en la red y su disponibilidad para cualquier usuario del recurso, acceso a internet sin restricciones y filtros, ejecución de comandos de acceso remoto desde cualquier terminal, etc.

F. Equipos de comunicación

Switch Catalyst 3560

- La Empresa Editora El Comercio S.A. Planta Norte cuenta actualmente con 3 switch Catalyst 3560 que soportan la interconexión directa de todos los host's y Servidores principales, de los cuales solo uno será configurado para trabajar como Switch Core.

G. Router Cisco 2800 Series

- Para el enrutamiento externo cuenta con 1 Router Cisco 2800 Series, donde si bien toda esta plataforma Lan permite la interconexión externa, no lleva implementado configuraciones avanzadas para trabajar a escalas superiores, brindando las características que debe tener una red como Escalabilidad, Tolerancia a fallas, Calidad de Servicio y Seguridad.

Cuadro N° 02: Distribución de los Equipos de comunicación para datos.

UBICACIÓN	EQUIPO	MODELO	VELOCIDAD	PTOS. OC.	PTOS. DISP.	CANT EQ.
Planta Norte	Router Cisco	2800 Series	100/1000 Mbps	1	3	1
Planta Norte	Switch Cisco	Catalyst 3560	10/100 Mbps	20	4	1
Planta Norte	Switch Cisco	Catalyst 3560	10/100 Mbps	21	3	1
Planta Norte	Switch Cisco	Catalyst 3560	10/100 Mbps	4	20	1

H. Hosts soportados

Representa la distribución de las computadoras en los departamentos de la Planta. Así mismo se consigna las Laptops designadas para algunos colaboradores.

Cuadro N° 03: Distribución de las PCs Planta Norte Diario El Comercio

Áreas	Computadoras				
	Laptop Core i3	Desktop Core 2 Dúo	Desktop Core i3	Servidor Intel Xeon	Total
Administración	2	6			8
Redacción		10			10
Pre prensa		1	3		4
Seguridad		1			1
Publicidad			3		3
Rotativa		4			4

Despacho		4			4
Circulación	1	6			7
Mantenimiento		4			4
Almacén	1	3			4
Sistemas				4	4

I. Inventario de software – El Comercio Planta Norte

CUADRO Nº 04: Software Prioritarios Utilizados.

Nombre del Programa	Proveedor	Licencias
Microsoft Office 2007	Microsoft	Licenciado
Microsoft Office 97	Microsoft	Licenciado
Paquete Adobe Professional	Microsoft	Licenciado
KaspersKy	KaspersKy	Licenciado
SAP	SIPSA	Licenciado
Arkitex	Agfa	Licenciado
Windows Server 2008	Microsoft	Licenciado
Windows 2000 Workstation	Microsoft	Licenciado
SQLSERVER 2005	Microsoft	Licenciado
DTI	D DTI	Licenciado
Excalibur Manager	Agfa	Licenciado
Windows X Profesional	Microsoft	Licenciado
Windows Server 200	Microsoft	Licenciado
Windows Seven Ultimate	Microsoft	Licenciado
PrintPlank	KMR	Licenciado
ECRM RIP	Arlequin Rip	Licenciado
PrintPlotter Manager	Agfa	Licenciado
Corel Drawn X3	Corel Corporation	Licenciado

J. Calidad de Servicio

Se ha determinado que los equipos de comunicación instalados tienen la capacidad de soportar la implementación de tecnologías que mejorarán el rendimiento y seguridad en la red como por ejemplo: VLAN, ACL, QoS, etc.

4.2. Análisis de Factibilidad

a) Factibilidad Operativa

Para poner en marcha este proyecto en la Empresa Editora El Comercio Planta-Norte, no es necesario contratar personal adicional al existente, considerando que si se llegase a implementar la propuesta, esta sólo afectaría los controles internos o niveles lógicos, cambios en los parámetros de configuración, implementación de nuevos protocolos, etc.

El personal operativo, llevará a cabo sus tareas o actividades de la misma manera en la que ha venido haciéndolo, considerando que es personal calificado y adaptable a cambios tecnológicos (uno de los requisitos de la empresa). Por ello, la factibilidad operativa es dable en este contexto.

b) Factibilidad Técnica

La plataforma tecnológica si bien está trabajando y soportando múltiples procesos, está aún no ha llegado al tope de su capacidad operativa, debido a que las características técnicas que presentan (Equipos de comunicación Cisco switches Catalyst 3560, Router 2800 Series, Procesadores Core 2 Dúo, Core i3, Intel Xeon, Cableado estructurado con certificación de calidad, etc.) aún no han sido dispuestas desde un enfoque estratégicamente acorde a la nueva realidad problemática.

El mercado hoy ofrece nuevas tecnologías, métodos y procedimientos para abordar las nuevas exigencias de la empresa, contando para ello con los conocimientos técnicos necesarios para la implementación de una plataforma lógica robusta, confiable y sostenible en el tiempo.

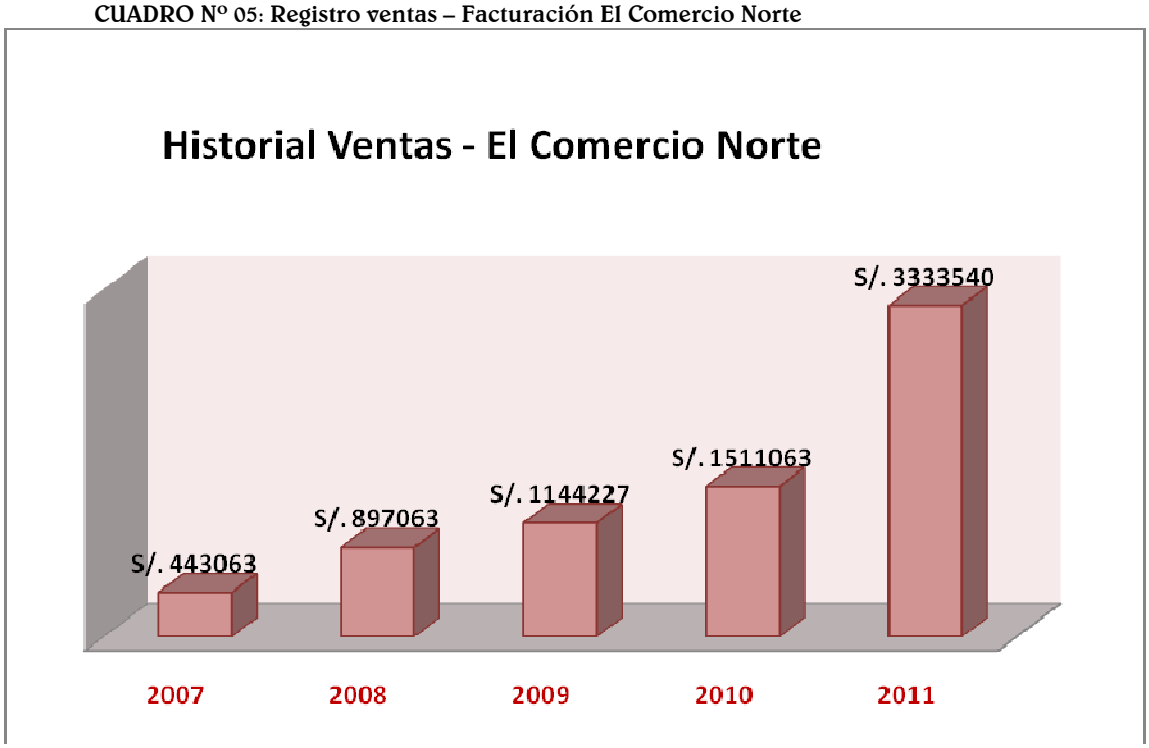
c) Factibilidad Financiera

La empresa Editora El Comercio S.A. – Planta Norte cuenta con disponibilidad económica para sustentar el desarrollo e implementación de este proyecto de investigación.

Considerando además que en los últimos 5 años las ventas se han incrementado exponencialmente, gracias a la apertura de mercado del Nororiente.

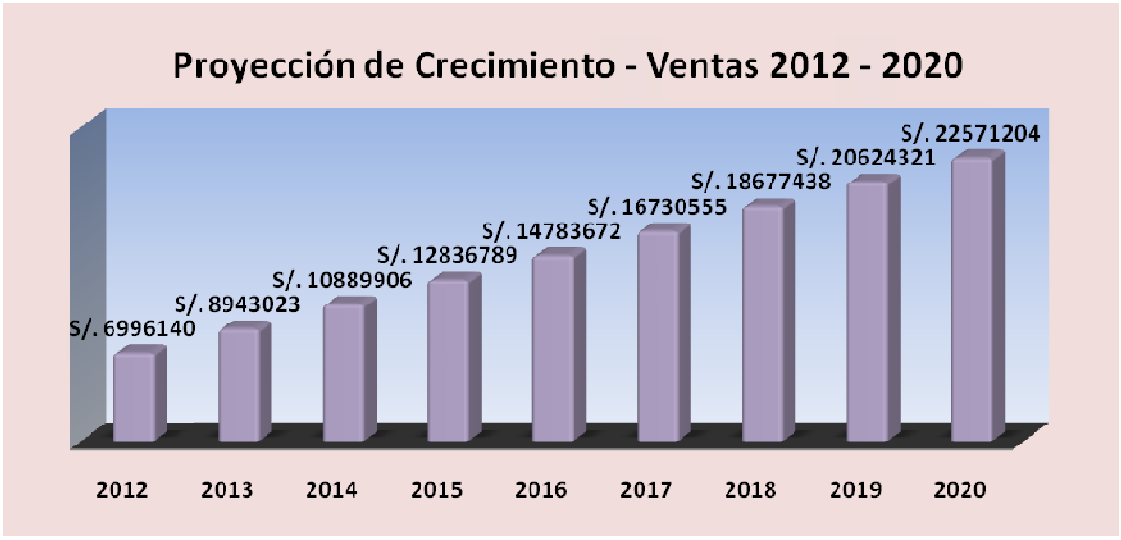
Por ello al estar en crecimiento tanto económico como de procesos es importante que esta se vea apoyada en el uso de nuevas tecnologías para así fortalecer el plan de negocio, contando asimismo con la aprobación o visto bueno de un presupuesto destinado a mejoras tecnologías por parte del Sr. Aníbal Cáceres Santín – Jefe Regional Grupo El Comercio Planta Norte.

CUADRO Nº 05: Registro ventas – Facturación El Comercio Norte



Fuente: Registro de Ventas de la Empresa al mes de agosto del 2011 Zona Norte.

CUADRO Nº 06: Proyección de ventas –El Comercio Norte



Fuente: Proyección de Ventas de la Empresa El Comercio Planta Norte.

4.2.1. Fase II: Análisis de Datos y Requisitos

4.2.1.1. Análisis de la Red actual de la empresa editora El Comercio Planta Norte.

La red de la empresa editora El Comercio Planta Norte, cuenta con las siguientes características:

- La red presenta una topología Estrella pero es plana en su diseño lógico lo cual representa varias desventajas, incluyendo un único dominio de broadcast de Capa 2 como, por ejemplo, una petición ARP, viaja hacia cada host y dispositivo en la LAN, estos y otros broadcasts de capa 2 consumen una gran cantidad del ancho de banda disponible de la LAN, ello aunado al vertiginoso volumen de información que se da entre host durante horas pico que logran generar "cuellos de botella".

- La asignación de IP's privados en cada Pc es manual, seguidos por un orden consecutivo (192.168.1.1, 192.168.1.2, 192.168.1.45, …)

- Debido a su diseño lógico brinda menor flexibilidad en el tráfico de red y la seguridad. No existe ningún control sobre la ruta de las tramas. La fiabilidad es baja, debido a que no se tiene disponibilidad de la red al 100% durante las 24 horas.

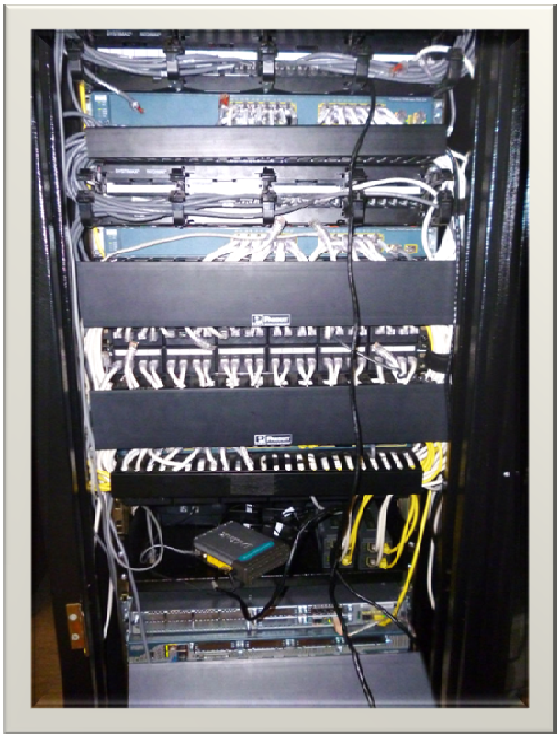
- Las características técnicas de los dispositivos de conectividad son de un alto nivel, como es el caso de los switches modelo Catalyst 3560, Router modelo 2800 Series, que poseen la capacidad suficiente para soportar las altas exigencias que hoy en día soporta la red. Sin embargo no existe una administración más rigurosa de estos equipos.

- El cableado estructurado esta implementado de acuerdo a las normas de calidad, respetando así espacios entre distintos enlaces, canaletas correctamente ubicadas, etc., presentando para ello un certificado de garantía.

- Se cuenta con un estabilizador "Emerson Network Power" con capacidad de proveer energía a 100 equipos de comunicación durante 1 hora (Pc's, Teléfonos IP, Impresoras, Routers, Switches, etc.) y a su vez brindar corriente estabilizada evitando así el aumento o baja intempestiva de la energía eléctrica.

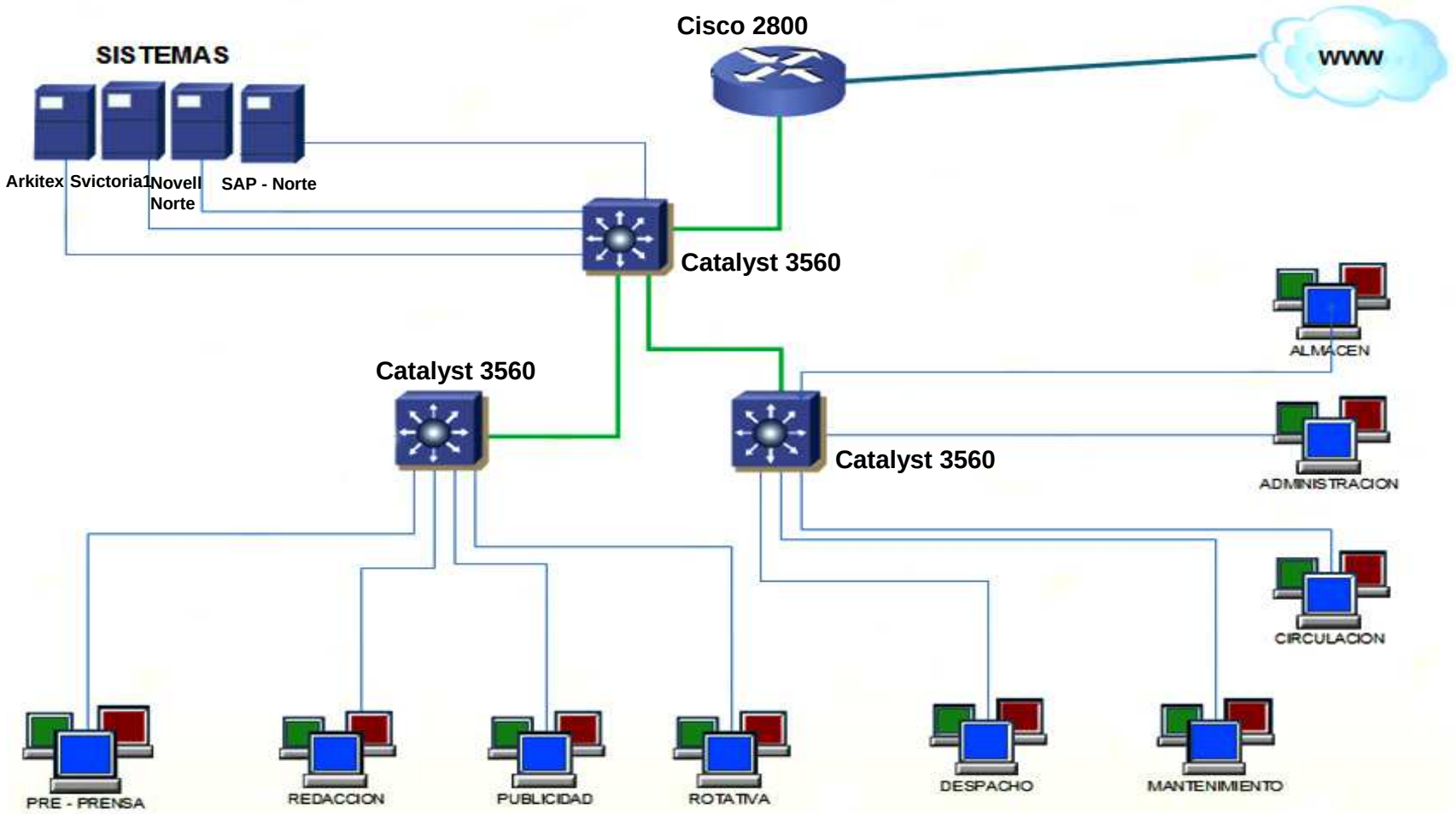
- No existen políticas de seguridad rigurosa y acorde a los nuevos procesos de trabajo.

Figura Nº 21: Imagen del gabinete de los equipos de comunicación Planta Norte



Conjunto de dispositivos que soportan la interconexión de la empresa, basada en equipos de la familia Cisco, ubicada en el área de Sistemas.

Figura Nº 22: Red actual de la empresa editora El Comercio Planta Norte.



4.3. Análisis Rendimiento de la Lan.

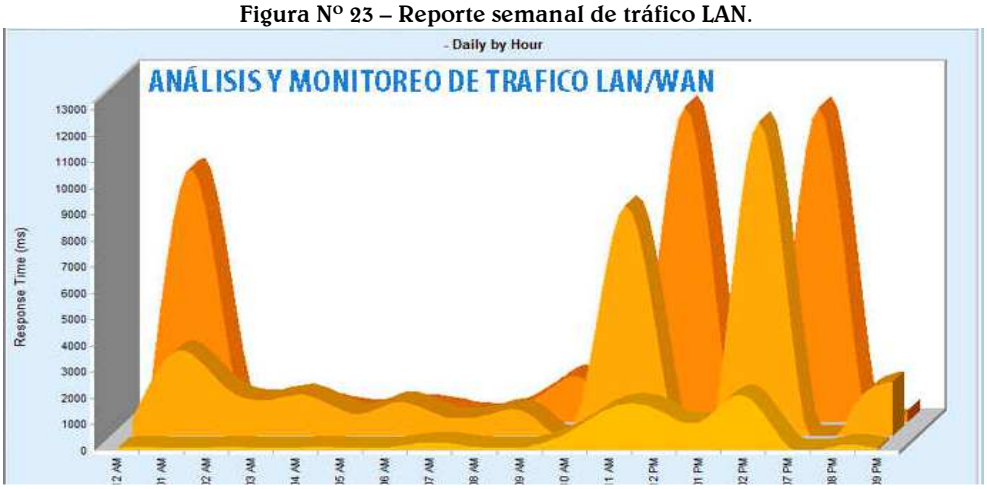
Se realizó el análisis del tráfico de red en la empresa editora el Comercio S.A. – Planta Norte, la cual gracias a las herramientas de análisis de rendimiento LAN, permitieron obtener resultados que grafican el estado actual de la red. El promedio ideal o esperado del tráfico fluctúa entre los 8 MB/s a 10 MB/s, siendo el objetivo primordial medir el rendimiento, observar cuan congestionada esta nuestra red, y emplear mecanismos para evitar el mal rendimiento.

Una de las causas de congestión que se determino son las siguientes:

- Velocidad insuficiente de las líneas.
- Ausencia de estrategias QoS.
- Interfaces de baja velocidad en los enlaces troncales.
- Protocolos IPX presentes en Pc's de manera innecesaria por tema de usabilidad.

Para poder obtener el rendimiento real de la red; se ha utilizado el software **PTRG NETWORK MONITOR**.

Figura Nº 23 – Reporte semanal de tráfico LAN.



Fuente: Gráfico obtenido del área de Sistemas Planta Norte El Comercio - PTRG

Descripción. En la figura Nº 03 observamos que durante las horas 12 am y 1 am existe una mayor saturación en nuestra red local, originando un tiempo de retardo mayor en las transacciones que están fluyendo, esto se debe a que los enlaces no pueden administrar una gran cantidad de información.
También se observa que entre las horas 7:00 am a 10:00 am existe un tráfico de red menor, lo que permite que la red trabaje de manera fluida sin percances o saturación.
Del mismo modo se detalla que entre las 11 am y 9 pm el tráfico aumentó de manera exponencial, ocasionando un bajo rendimiento de la Lan, todo ello muestra que la infraestructura tecnología de comunicación no cumple con el estándar adecuado de velocidad.

4.4. Análisis de Seguridad de la Red.

El activo más importante en las organizaciones públicas, privadas y de cualquier índole, es la información que tienen. Entre más grande es la organización más grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia brindar todas las garantías necesarias a la información o Data.

Dentro del entorno de la red de la empresa editora El Comercio S.A. – Planta Norte, se detectaron los posibles puntos vulnerables:

- Falta de políticas de seguridad en la red interna, como permisos y restricciones hacia los dispositivos intermediarios de red.
- Falta de parametrización en el acceso a los recursos compartidos.
- Ausencia de ACL's (Lista de control de acceso) para el filtrado de paquetes de forma externa e interna.
- No existe un servidor de autenticación para el acceso, control y administración de los dispositivos intermediarios de red.
- Acceso de "extremo a extremo" no controlado.
- Acceso no controlado a los servicios de internet.
- Falta de mecanismos de aislamiento y protección a los dispositivos finales.
- Ausencia de mecanismos de control y administración en el almacenamiento de archivos.
- El Router principal no cuenta con seguridad avanzada.

Figura N° 24. Diagrama Intruso

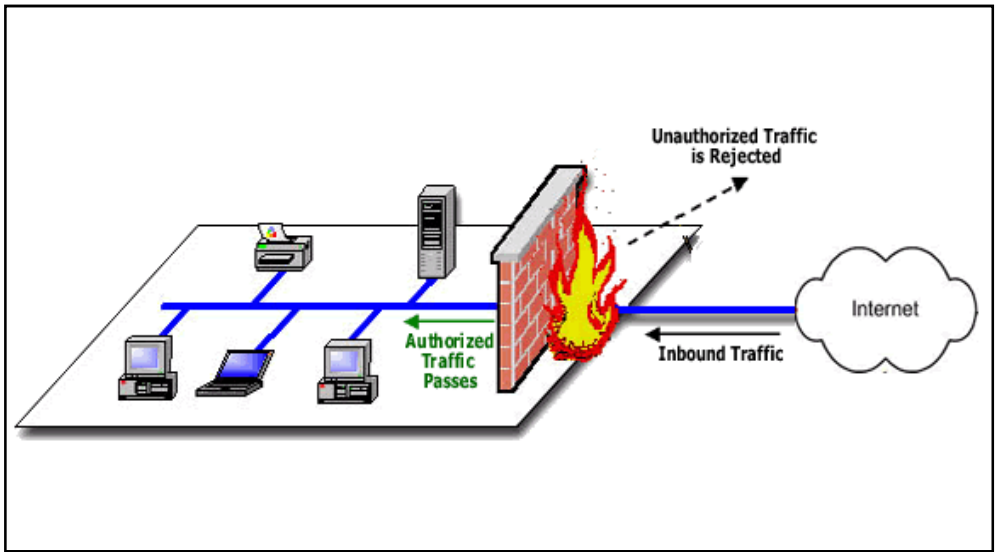
Fuente: cisco.netacad.net/Academy

4.5. Análisis de los Requerimientos

4.5.1. Firewall Cisco ASA 5520 (Dispositivo seleccionado como parte de la propuesta)

Dispositivo que funcionara como cortafuegos entre redes, permitiendo o denegando las trasmisiones de una red a la otra. Sera situado entre la red local y la red Internet como dispositivo de seguridad para evitar que los intrusos puedan acceder a la red interna.

Figura N° 25. Funcionamiento de Firewall



Fuente: cisco.netacad.net/Academy

Cumplirá las siguientes funciones:

0 Filtrado de Paquetes.
1 Implementación de ACL.
2 Permisos y restricciones en determinados puertos, etc.

Figura N° 26. Firewall ASA 5520 – Dispositivo seleccionado

Fuente: www.cisco.com/en/US/products/

Cuadro N° 07: Características técnicas del Firewall ASA 5520

Descripción del producto	Cisco ASA 5520 Firewall Edition - aparato de seguridad
Tipo de dispositivo	Aparato de seguridad
Tipo incluido	Montable en bastidor - 1U
Dimensiones	44.5 cm x 33.5 cm x 4.4 cm
Peso	9.1 kg
RAM instalada (máx.)	2 GB
Memoria flash instalada	256 MB Flash
Protocolo de interconexión de datos	Fast Ethernet, Gigabit Ethernet
Red /Protocolo de transporte	IPSec
Rendimiento	Capacidad del cortafuegos : 450 Mbps Capacidad de la VPN : 225 Mbps Tasa de conexiones : 9000 sesiones por segundo
Capacidad	Sesiones concurrentes : 280000 Peers VPN IPSec : 750 Peers VPN SSL : 2 Interfaces virtuales (VLAN) : 100
Características	Protección firewall, asistencia técnica VPN, equilibrio de carga, soporte VLAN
Alimentación	CA 120/230 V (50/60 Hz)

4.5.2. Otras alternativas de Firewall en el mercado.

Además del firewall seleccionado para la propuesta de implementación, se tuvo en cuenta otras marcas y características técnicas diferenciadoras que permitieron la elección, como las siguientes:

Figura N°: 27 FIREWALL PIX CISCO 500

Fuente: www.cisco.com/en/US/products/

Cuadro Nº 08: Características firewall pix cisco 500

Velocidad de transferencia de datos	60 Mbit/s
Características de red	LAN,WAN,VPN
p Protocolo de trasmisión de datos	X.509 ,PPPoE,NAT/PAT ,SCCP,ILS,RTSP
Protocolos de gestión	SNMP
Algoritmo de Seguridad	56-bit DES, 168-bit 3DES and up to 256-bit AES data-encryption to ensure data privacy
Método de autenticación	TACACS+ ,RADIUS
Interfaz	RJ-45
Tecnología de conectividad	Ethernet/FastEthernet
Memoria interna, mínimo (RAM)	8 MB
Memoria flash, mínimo	16 MB
Software incluido	Cisco IOS
Velocidad de reloj	133 MHz

Firewall GTA GB

Figura N° 28 GTA/GB-800 Firewall/VPN

Fuente: www.cisco.com/en/US/products/

Cuadro Nº 09: Características Firewall GTA GB

Licencias para 50 usuarios o usuarios ilimitados
▪ Segmentación de la red en 3 subredes (LAN, DMZ, Externa)
▪ Soporte opcional para Mail Sentinel AntiSpam y Mail Sentinel AntiVirus
▪ El modelo GB-800e incluye aceleración de VPN por hardware
▪ Administración a traves de páginas de web, programa de administración para Windows (gratuito al comprar el equipo), o emulador de terminal VT-100 con cable serie null-modem de 9 pins
▪ Alta disponibilidad de acceso (múltiples conexiones a Internet o ISPs)
▪ Alta disponibilidad de hardware opcional (cluster de 2 equipos GB-800 con la opción H2A)

Firewall 3COM

Figura N° 29: **Firewall 3com**

Cuadro Nº 10: Características Firewall 3com

Transmisión de datos	
Firewall throughput	500 Mbit/s
VPN throughput	60 Mbit/s
Red	
DHCP, servidor	Si
Protocolos	
Protocolos de gestión	HTTP, HTTPS, SSH & SNMPv2c
Protocolos de red admitidos	HTTP, IPSec, L2TP, PPPoE, PPTP, TCP/IP, UDP/IP, TCP, HTTPS
Protocolo de routing	RIP, Static Routing, DynDNS
Seguridad	
Algoritmo de seguridad	DES, 3DES, AES, MD5, IKE, SHA-1
Método de autenticación	PAP (UPAP), CHAP, SHA-1, MD5
Firewall, seguridad	SPI, DoS, URL Filtering, NAT
Conectividad	
Tecnología de conectividad	Con cables
Características del puerto WAN	Si
Ethernet DMZ ports quantity	2
Puertos de entrada y salida (E/S)	WAN: 2 x 10BASE-T/100BASE-TX/1000BASE-T LAN: 6x 10BASE-T/100BASE-TX/1000BASE-T RJ45
Peso y dimensiones	
Dimensiones (Ancho x Profundidad x Altura)	330 x 203 x 44 mm
Peso	1500 g

Observación:

Por que elegir Firewall Físico respecto del Firewall Lógico

Análisis de tipo de elección.

Si bien un **firewall lógico** constituye una alternativa más económica en relación con los firewall basados en hardware, sin embargo presentan mayores desafíos en su implementación.

- Debe seleccionarse adecuadamente la plataforma de hardware y endurecer el sistema operativo, para realizar reenvío de paquetes.
- Corren por defecto servicios que no son requeridos si la máquina funciona como firewall exclusivamente.
- Su arquitectura es menos robusta y especializada para operar como analizador de paquetes.
    - Consume recursos del computador que lo aloja.

Algunos ejemplos de firewalls basados en software son los siguientes:

- Checkpoint(Virtualizado)
- IPTables
- Microsoft Internet Security & Aceleration Server
- Untangle
- SmoothWall
- Engarde Secure Linux
- M0n0wall

Por ello la elección de un firewall Físico como parte de la propuesta de implementación obedece a que estos dispositivos fueron concebidos íntegramente para mitigar ataques, puesto que su arquitectura fue diseñada para ello.

- También muestran un mejor desempeño en comparación con los firewalls basados en software.
- Menor tiempo de implementación que los firewalls basados en software.
- Reducen necesidad de decidir entre hardware, sistema operativo y software de filtrado, ya que todo viene configurado, simplificado y optimizado en un solo paquete.

4.6. Servidor AAA – Radius

Es un protocolo de autorización y autentificación para aplicaciones de acceso a red, utiliza el puerto 1812 UDP, a su vez facilitara la administración de usuarios y su acceso a dispositivos de red, se encargara de reforzar la seguridad a nivel lógico.

Cumplirá las siguientes funciones:

- Servicio de Autenticación y Encriptación a un cliente: **El Router RCOMERCIO.**
- Usuarios y contraseñas personalizadas por cada cliente.
- Uso de certificados de Windows para asegurar la autenticación.

Asimismo se utilizara el Sistema Operativo WINDOWS SERVER 2008 para configurar nuestros clientes Radius y nuestras cuentas de acceso estarán disponibles en un nuevo grupo de Active Directory del mismo sistema.

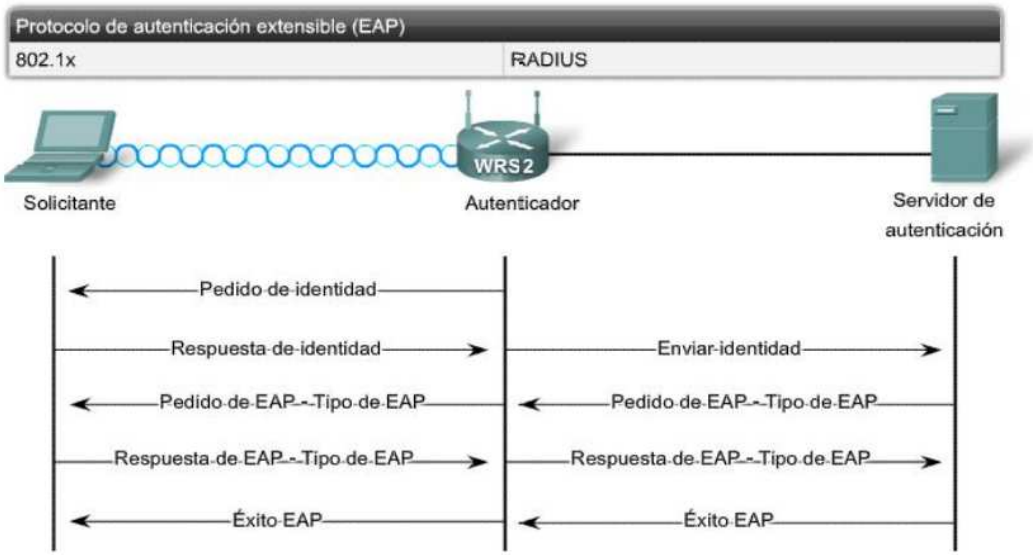
Descripción de las tres funciones que cumplirá el Servidor Radius:

Autenticación
Mediante este proceso una entidad prueba su identidad ante otra. La primera entidad es un cliente (usuario, ordenador, etc.) y la segunda un servidor (ordenador).

Autorización
Se refiere a la concesión de privilegios específicos a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema.

Contabilización
Mostrara un seguimiento del consumo de los recursos de red por los usuarios. Esta información se utilizara posteriormente para la administración, planificación, facturación, u otros propósitos.

Figura N° 30: Funcionalidad Servidor Radius

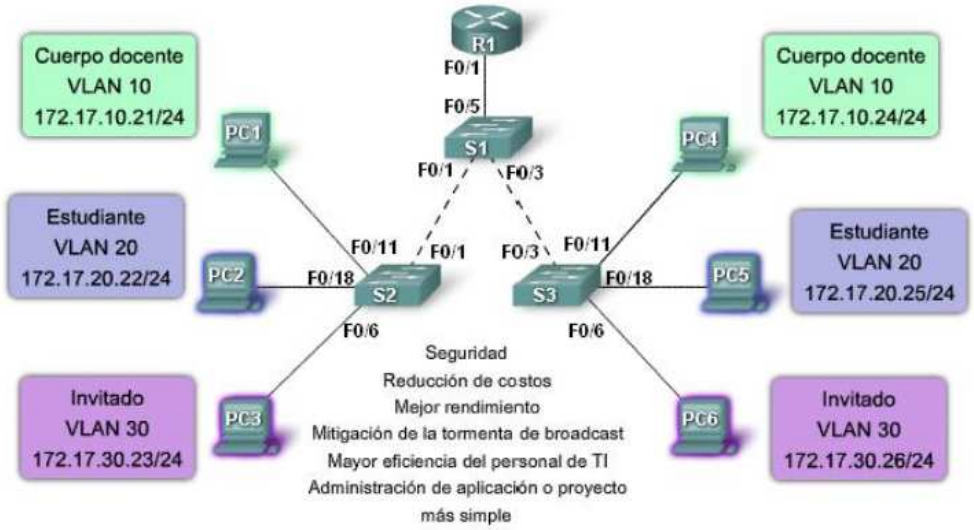


Fuente: Manual Administración Redes Cisco Networking 2011.

4.7. Redes Virtuales (VLAN)

Nuestra red pretende presentar configuración e implementación de redes de área local virtuales, para mejorar el rendimiento de la red, proveer seguridad, segmentación, mejor administración de red, reducción de costos, uso adecuado y jerárquico cumpliendo con todas los estándares de red. La infraestructura tecnológica con que se cuenta dentro de las instalaciones de la empresa, permite soportar Redes Virtuales, permitiendo así implementar toda la gama de configuraciones para mejorar el desempeño de la LAN.

Figura N° 31: Interconexión VLAN



4.8. Identificación de las alternativas

Si bien los equipos que soportan las comunicaciones de la empresa Editora El Comercio Planta Norte; son de la **Familia CISCO**, también existen otras marcas líderes en el mercado, como:

- **3COM (HP)**
- **AVAYA.**
- **D-Link**
- **ENCORE**

La empresa editora el Comercio cuenta con un diseño estructurado utilizando tecnología CISCO, y por ello no es pretensión cambiar los equipos por otras marcas o modelos de las mismas, sino todo lo contrario; la idea es utilizar los dispositivos con que contamos y elevar su nivel de trabajo mediante estrategias e implementaciones lógicas y físicas, para de esta manera obtener mejores resultados que los actuales.

Los equipos de Red son los siguientes:

- **Router Cisco 2800 series** – **Cantidad : 1**
- **Switch Cisco Multilayer 3560** – **Cantidad : 3**
- **Teléfonos IP cisco 7941** – **Cantidad : 15**

Cuadro Nº 11: Comparaciones entre equipos CISCO Y 3COM

Tomaremos ejemplos en 2 modelos similares en switches:

Información de Configuración	Switch Cisco 2960 24 ptos 10/100 Mbps + 2 ptos Gbps	Switch 3Com (HP) SS 3 4300 24 ptos 10/100 Mbps
Redundancia		
Protocolo Spanning Tree	Si	Si
PortFast (Puertos Rápidos)	Si	No
Backbones Fast	Si	No
Tecnología PVST + para enlaces troncales	Si	No
Optimización de Ancho de Banda		
Fast/Gigabit EtherChannel	Si	Si
VTP (Protocolo troncal de VLAN)	Si	No
VLAN VOZ	Si	No
QoS (Calidad de Servicio)		
Prioridad de VLANS	Si	No
Configuración de QoS por puerto	Si	No
Seguridad		
Seguridad de Puertos	Si	No
Notificación de direcciones MAC	Si	Si
Autenticación por servidores Radius o Tacacs	Si	No

- La tecnología Cisco predomino en la mayoría de parámetros y por lo consiguiente la empresa editora el Comercio no debe migrar su tecnología hacia otras marcas.

4.8.1. FASE III. Diseño de la Solución

4.8.1.1. Diseño de la Estructura Lógica

Criterios

De acuerdo a los lineamientos de desarrollo que queremos alcanzar para un correcto rediseño lógico, nos basamos en 4 criterios fundamentales:

- Seguridad
- Funcionalidad
- Escalabilidad
- Adaptabilidad

El objetivo principal es mejorar el Rendimiento y Seguridad de la plataforma LAN que soporta los procesos en la Empresa Editora El Comercio Planta Norte, para ello los 4 criterios serán los pilares para esta propuesta.

a) **Seguridad.**

- **Radius**, gracias al servidor Radius se permitirá controlar los accesos a los recursos de la Lan, tanto externo como interno. Como por ejemplo el ingreso hacia la granja de Servidores de la empresa estará parametrizada en la BD y políticas del Radius.

- **ACL**, la red mantendrá la seguridad a nivel lógico con la creación de reglas de acceso, que permitirá generar restricciones a los terminales de diferentes áreas disminuyendo la vulnerabilidad de los datos que fluyen.

- **Tecnologías Seguridad Emergentes**: **NetWork Access Protection**, que establece Redes de cuarentena ante cualquier infección o ataque interno y **File Screening Management** que bloquea el almacenamiento en el servidor de archivo no autorizados como música, videos, etc.

- Se aplicara la instalación de un Firewall Físico, modelo **Firewall CISCO ASA 5520** para el filtrado de paquetes entrantes y salientes, reforzando de esta manera la protección en la Lan.

b) **Funcionalidad.**

La red proporcionará conectividad de usuario a usuario a través de la red, y de usuario a aplicación con una velocidad y confiabilidad muy razonable.

- **VLAN**, mediante la segmentación de la LAN en subredes, permitirá crear fronteras lógicas para los distintos departamentos, aumentando los niveles de seguridad.
- Las conexiones de host de la red es de 10/100 Mbps
- Se implementara **enlaces troncales de 1GB** más la aplicación de protocolo **LACP** que incrementara la tasa de transferencia del enlace físico.
- Se implementara un Acces Point para el acceso inalámbrico desde cualquier punto de la Planta.
- La red será **sensible a QoS** para así efectuar la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación.

- La red actual cuenta con la asignación de IP de manera manual, donde el control es consecutivo: 192.168.1.1 – 192.168.1.xx…. Ante este panorama se implementara un **Servidor DHCP** para la asignación automática de IP en todos los dispositivos finales de la LAN, todo ello será implementado en el Router Cisco 2800 Series, bajo los parámetros de rango de cada Vlan.

c) Escalabilidad.

La red podrá aumentar su tamaño, sin que ello produzca cambios importantes en el diseño general por lo que se proveerá de un número considerable de puntos de red. Los Switches son escalables para permitir aumentar la cantidad de puertos para soportar crecimientos futuros.

d) Adaptabilidad.

La red estará rediseñada teniendo en cuenta las diferentes tecnologías y sus diferentes aplicaciones normativas lo que garantizará una amplia adaptabilidad muy independiente de la tecnología que se llegase a implementar.

4.9. Estructura Modelo Jerárquico de 3 Capas – Metodología Cisco

4.9.1. Capa de acceso

La implementación de esta capa (Física) cuenta con **certificación de calidad y garantía por una empresa privada**, lo que involucra que el cableado estructurado se encuentra en perfectas condiciones, brindando la seguridad de no anomalías bajo esta naturaleza. Las tarjetas de red de los dispositivos finales están 100% operativas.

4.9.2. Capa de distribución

Aquí se establece el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar las siguientes funciones:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Proporcionar servicios de seguridad y filtrado.

- Proporcionara conectividad basada en una determinada política.
- Asimismo este nivel se encargara del direccionamiento hacia los nuevos Servidores propuestos como: **FTP** (Alojado en Servidor de Datos SVICTORIA1), **Radius** (Alojado en Servidor Arkitex), **DHCP** (Alojado en el Router Cisco 2800 Series)

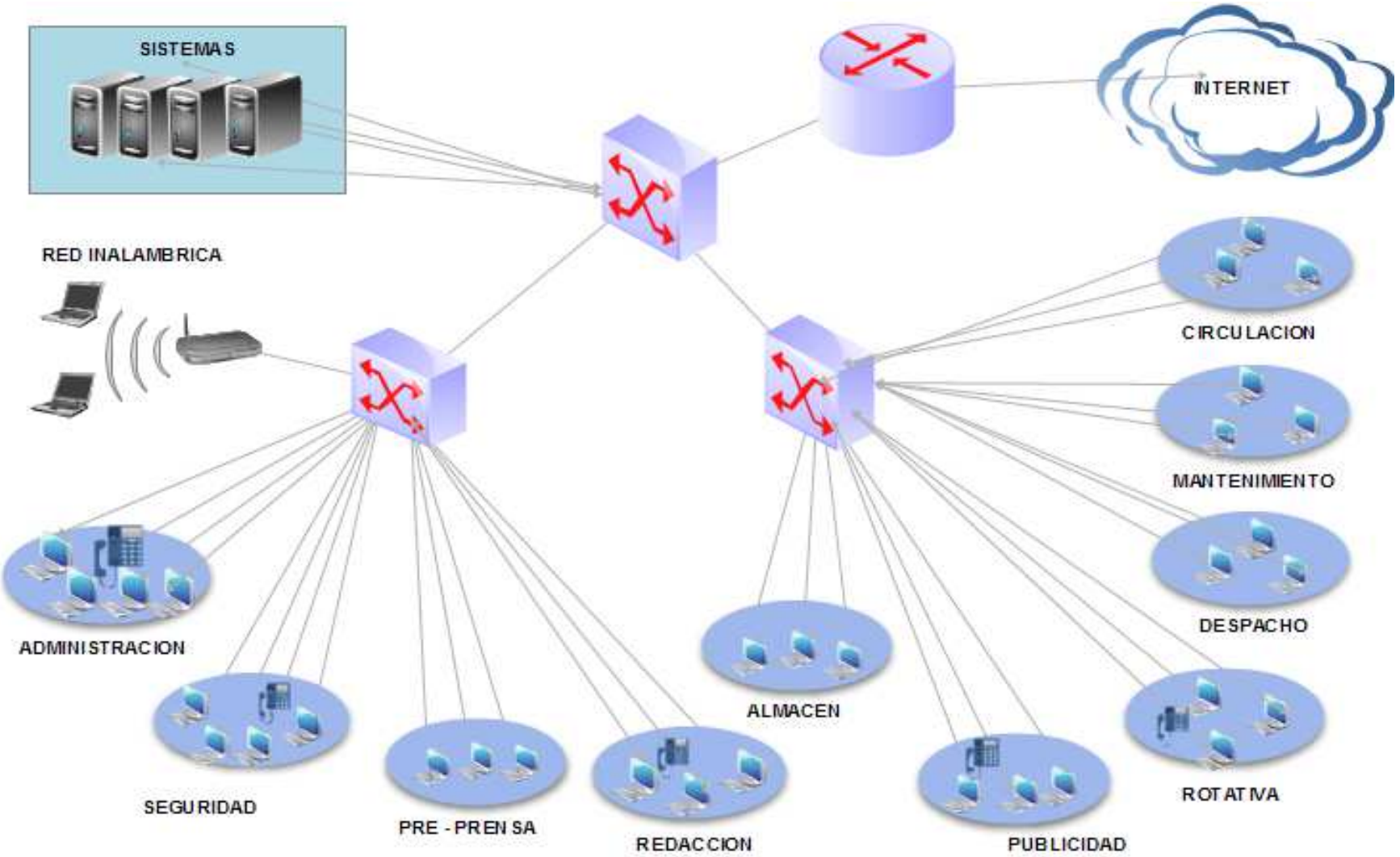
4.9.3. Capa de Núcleo

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos.

Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución.

El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

Figura N° 32: Segmentación de áreas mediante VLAN's.- Se contara 14 VLAN y 2 enlaces WAN, teniendo un total de 16 subredes.



- Cuadro Nº 12: Tabla de direccionamiento IP propuesto

	DIRECCIÓN DE RED	RANGO DE DIRECCIONES IP	MASCARA DE SUBRED	Nº Host Propuestos	Nº Host Ocupados	Nº Host Libres	ÁREA
1	172.16.1.32	172.16.1.33 – 172.16.1.62	255.255.255.224	**29**	**10**	**19**	**REDACCIÓN**
2	172.16.1.64	172.16.1.65 – 172.16.1.78	255.255.255.240	**13**	**8**	**5**	**ADMIN - COMERCIO**
3	172.16.1.80	172.16.1.81 – 172.16.1.94	255.255.255.240	**13**	**6**	**7**	**CIRCULACIÓN**
4	172.16.1.128	172.16.1.129 – 172.16.1.134	255.255.255.248	**5**	**3**	**2**	**PRE PRENSA**
5	172.16.1.136	172.16.1.137 – 172.16.1.142	255.255.255.248	**5**	**4**	**1**	**ROTATIVA**
6	172.16.1.144	172.16.1.145 – 172.16.1.150	255.255.255.248	**5**	**4**	**1**	**DESPACHO**
7	172.16.1.152	172.16.1.153 – 172.16.1.158	255.255.255.248	**5**	**4**	**1**	**MANTENIMIENTO**
8	172.16.1.168	172.16.1.169 – 172.16.1.174	255.255.255.248	**5**	**3**	**2**	**PUBLICIDAD**
9	172.16.1.96	172.16.1.97 – 172.16.1.110	255.255.255.240	**13**	**4**	**9**	**SISTEMAS**
10	172.16.1.160	172.16.1.161 – 172.16.1.166	255.255.255.248	**5**	**3**	**2**	**ALMACÉN**
11	172.16.1.176	172.16.1.177 – 172.16.1.182	255.255.255.248	**5**	**1**	**4**	**SEGURIDAD - PLANTA**
12	172.16.1.184	172.16.1.185 – 172.16.1.186	255.255.255.252	**1**	**1**		**ENLACE WAN 1 ROUTER-FIREWALL**
13	172.16.1.188	172.16.1.189 – 172.16.1.190	255.255.255.252	**1**	**1**		**ENLACE WAN 2 (INTERNET)**
14	172.16.1.0	172.16.1.1 – 172.16.1.30	255.255.255.224	**29**	**16**	**13**	**VOZ**
15	172.16.1.112	172.16.1.113 – 172.16.1.126	255.255.255.240	**26**		**26**	**INVITADO/Wifi**

- **Direccionamiento adicional (Para futuras áreas)**
  - **172.16.1.192/27**
  - **172.16.1.224/27**

4.10. Diseño de la Estructura de Seguridad

4.10.1. Acceso a Páginas de Internet.

Se implementara un servidor **proxy Jana 2.4** el cual permitirá compartir una conexión, es decir, ofrecer acceso a otros equipos de la red mediante una "conexión proxy", redireccionando la información (generalmente, páginas Web solicitadas por los equipos de la LAN). Este aplicativo estará alojado en el **Controlador de Dominio Arkitex** y administrado por el área de Sistemas.

Figura N° 33 Interfaz maestra del aplicativo Jana Server

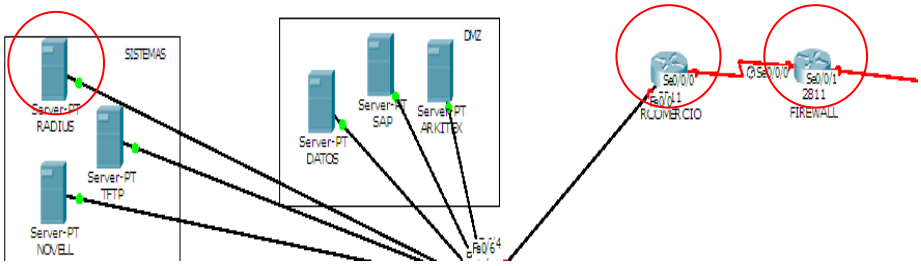
Fuente: Área Sistemas Diario La Industria de Chiclayo.

4.10.2. Implementación de un servidor AAA Radius

El Servidor AAA RADIUS permitirá la autenticación de los clientes tanto internos (LAN) como externos (WAN), solicitando usuario, contraseña y certificado de Windows para poder administrar remotamente el Router RCOMERCIO y de forma segura, afianzando el nivel de seguridad.

- Este aplicativo estará alojado en el Controlador de Dominio de la empresa, bajo la plataforma Windows Server 2008 R2.

Figura N° 34. Dinámica de funcionamiento Servidor Radius



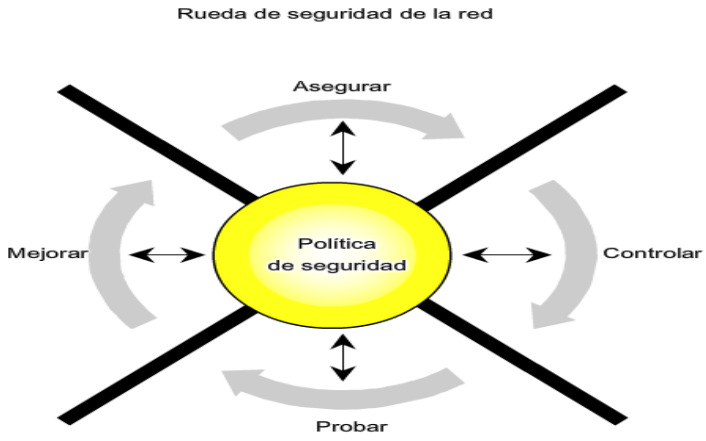
Fuente: Packet Tracert – Proyecto Red Lan El Comercio Norte

- Dicho router podrá ser administrado desde cualquier parte del mundo, siempre y cuando el solicitante este agregado en el servidor Radius, y el mismo reconozca su certificado de Windows para permitirle el acceso.
- Nuestro firewall y Servidor AAA RADIUS nos permitirán crear políticas de seguridad robustas, de confianza y acordes a las demandas de las redes actuales que nos permitan asegurar, mejorar y controlar todo el acceso absoluto de nuestra red.

Comandos de Configuración del Router RCOMERCIO (Router Cisco 2800 Series)

RComercio(config)#aaa new-model
RComercio(config)#aaa authentication login default group radius none
RComercio(config)#aaa authentication login telnet_lines group radius
RComercio(config)#radius-server host 172.16.1.99 auth-port 1645 key comercio
RComercio(config)#line vty 0 4
RComercio(config-line)#login authentication telnet_lines
RComercio(config)#

Figura N° 35. Políticas de Seguridad Redes Informáticas



Fuente: www.Cisco/netacad

4.10.3. Implementación de listas de control de acceso (ACL)

La seguridad se desplegará a través del uso de ACL (Access Control List).
En la empresa editora el Comercio, se han tomado en cuenta estrictas políticas de seguridad, y para ello se implementan Listas de Control de Acceso configuradas en nuestro Firewall.

Listado de ACL's:

- Solo las áreas de Redacción y Pre-Prensa pueden descargar archivos del servidor FTP. ACL extendida que bloquea el tráfico de FTP (El servicio FTP emplea el puerto TCP 21)
- Solo el Área de Sistemas podrá administrar de forma directa y remota el router principal RCOMERCIO.

Figura N° 36: Políticas de Seguridad Redes Informáticas

Fuente: Packet Tracert – Proyecto Red Lan El Comercio Norte

- No permitir el acceso remoto mediante el protocolo telnet a las áreas no autorizadas.
- ACL extendida que no permite el tráfico telnet (telnet es un servicio que usa el puerto TCP 23) desde cualquier estación a los servidores.ACL para permitir que cualquier host de una VLAN pueda enviar mensaje de correo electrónico (SMTP) a cualquier host de cualquier otra VLAN

4.11. Diseño de VLAN

Cuadro N° 13: Diseño de VLAN - Nuestra Red presenta las siguientes VLAN'S con sus respectivos ID y nombres.

ID de VLAN	Nombre VLAN	Cantidad de direcciones Ip actuales /PC	Cantidad de direcciones Ip propuestas / PC
10	SEGURIDAD-PLANTA	1 PC	5 PCS
20	PRE PRENSA	3 PCS	5 PCS
30	ADMI-COMERCIO	8 PCS	13 PCS
40	REDACCIÓN	10 PCS	29 PCS
50	PUBLICIDAD	3 PCS	5 PCS

60	ROTATIVA	4 PCS	5 PCS
70	DESPACHO	4 PCS	5 PCS
80	CIRCULACIÓN	6 PCS	13 PCS
90	MANTENIMIENTO	4 PCS	5 PCS
100	ALMACÉN	3 PCS	5 PCS
110	SISTEMAS	4 PCS	13 PCS
120	SISTEMAS	4 PCS	13 PCS
130	VOZ	16 TELEFONOS	29 TELEFONOS
140	INVITADO		26 PCS
99	ADMI-RED	VARIABLE	VARIABLE

Nuestra propuesta implementa Vlans (Redes virtuales de área local), lo que permitirá segmentar y/o dividir lógicamente nuestra red.
Las Vlans nos ofrecerán lo siguiente.

- Mejor Administración de la Red
- Mejor rendimiento de la red, reduciendo los dominios de Broadcast
- Seguridad a la red
- Administración de los dispositivos conmutadores (Switches) de forma remota.
- Permite implementar estrategias QoS, etc.

SWITCH CISCO 3560 – Red Lan El Comercio Planta Norte

Existen 3 switches Cisco modelo 3560 ubicada en el rack principal de la empresa, donde cada una de ellas actualmente cumplen la función de dispositivos que operan en la Capa de Acceso, por ello se designo a uno de ellos para trabajar como **Switch Core3.**

- Nuestro switch de capa 3, será el servidor VTP donde se crea, administra o elimina las VLan's, y estas mismas se replican hacia los switches 3560 que serán nuestros clientes VTP donde ellos no podrán crear, ni eliminar VLANS, solo accederán a las VLANS que requiera la empresa.

4.12. Tipo de VLAN: VLAN basada en puerto.

4.12.1. Estándar:

- **802.1Q**
  Nos va a permitir compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking).

- **Etiquetado de la Trama 802.1Q**
  Los switch solo utilizan la información del encabezado de trama para enviar paquetes.
  El encabezado no contiene la información que indique a que VLAN pertenece la trama.
  Posteriormente, cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen.
  Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q.
  Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

4.12.2. Protocolo:

VTP, para crear, administrar y eliminar VLAN

4.12.3. Hardware

Para soportar el esquema de VLAN tenemos los equipos:

1. Switch Cisco Catalyst 3560: Para la capa de distribución
2. Switch Cisco Catalyst 3560: Para la capa de acceso.

4.13. Implementación de Estrategias QoS (calidad de servicio)

La Red de la empresa editora el Comercio, posee una red de voz que debe de poseer la primera prioridad en el envío de datos.

- Las estrategias Qos nos permitirán identificar el tráfico de voz, y poder brindarle la prioridad a uno, lo cual indica que esa señal no puede esperar y debe ser transmitida de forma inmediata.

- Lo cual nos indica que nuestro switch está permitiendo el tráfico de 2 redes, una señal que es la de VOZ, y la otra que la de DATOS.

- Nuestro Switch debe de estar configurado para poder administrar estas señales para luego brindar prioridad.

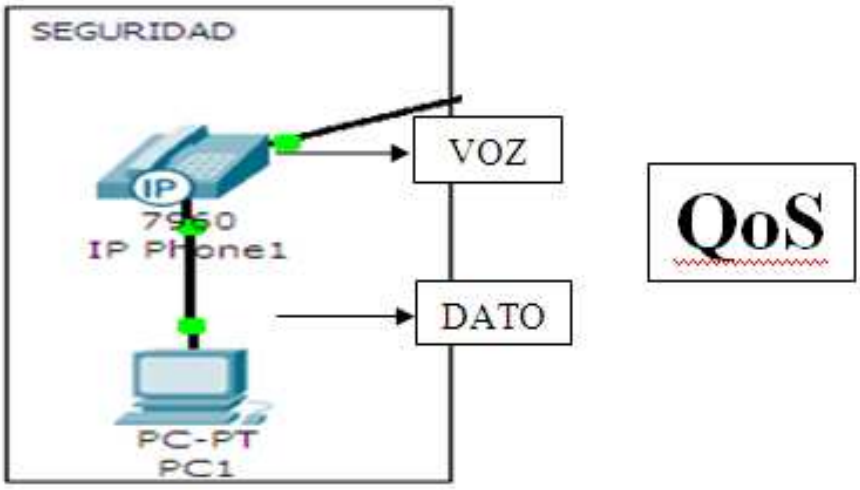
- QoS tambien estará implementado en 2 computadoras del área de Redacción, para tener prioridad de trafico al momento de transferir archivos "pesados" como videos (200 a 300 MB), conjunto de imágenes (120-150 MB), paginas o infografías (200 MB), etc.

Ejemplo de Configuración de QoS en los puertos del Switch

```
Interface FastEthernet0/2
switchport access vlan 10
```

switchport mode access
switchport voice vlan 120
mls qos trust cos
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
switchport voice vlan 120
mls qos trust cos

Las estrategias QoS están presentes en todo nuestro proyecto, y de esta manera también se nos permite ahorrar puertos en nuestro Switch.



A su vez el grafico nos indica que nuestro switch está permitiendo el tráfico de 2 redes, una señal que es la de VOZ, y la otra que la de DATOS.

4.14. Tecnologías de Seguridad Emergentes.

4.14.1. Implementación NetWork Access Protection

Mediante la implementación de NetWork Access Protection en el servidor Controlador de Dominio (Bajo Windows Server 2008) se pretende cubrir los siguientes puntos:

- Reforzar la política de seguridad y de salud en equipos portátiles, cuando éstos vuelvan a conectarse a nuestra red
- Restringir el acceso a nuestra red a todo equipo que no cumpla con la política de salud de la empresa.
- El estado de salud de un equipo será monitorizado por una parte del cliente NAP, denominado SHAs (System Health Agent).

- NAP verificará que las últimas actualizaciones de seguridad estén instaladas en el equipo, basándose en uno de los cuatro niveles de seguridad establecidos por la plataforma Microsoft Security Response Center (MSRT).

- Se dispondrá en la red de cuarentena de recursos que permitan actualizar los equipos con las últimas actualizaciones de seguridad, bases de virus, bases anti-spyware, y otros.

4.14.2. File Screening Management

Gracias a la implementación del aplicativo en el Servidor de Datos, se restringirá el almacenamiento de material que no esté bajo la línea de producción del diario, es decir materiales como música, archivos ejecutables, etc., todos ellos de naturaleza personal.
Específicamente usaremos esta funcionalidad para:

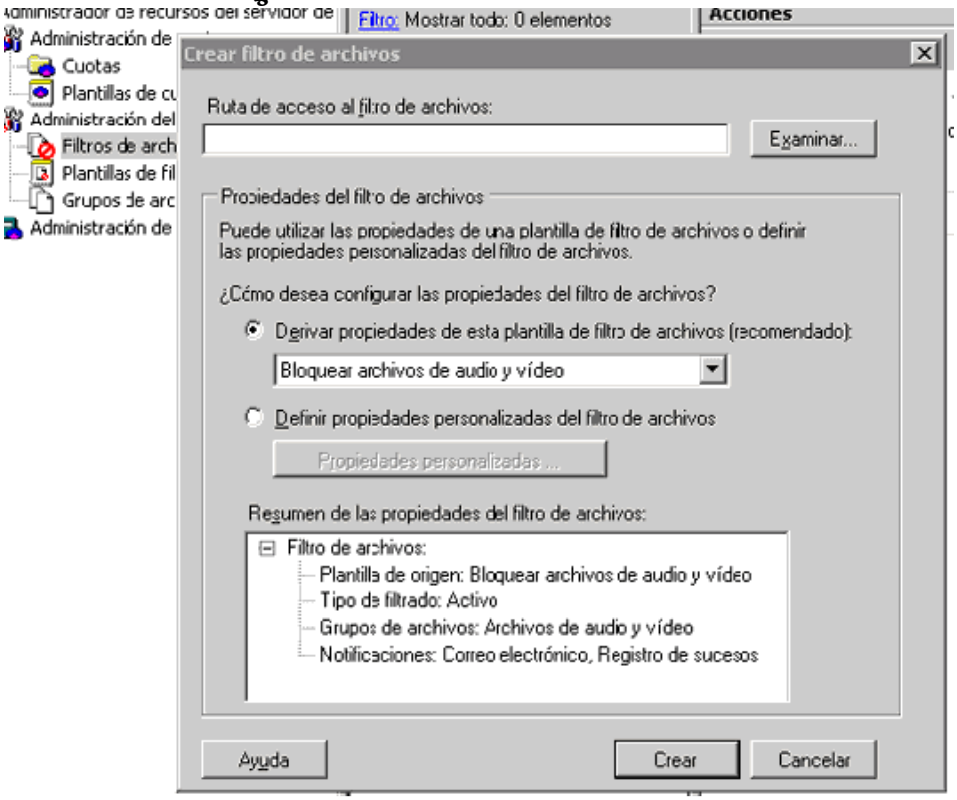
- Gestionar cuotas de forma que se establezcan una serie de límites de espacio sobre un volumen o árbol de directorios.

- Filtros o restricciones personalizadas para extensiones de archivos ("file screening") de esta manera definimos reglas para monitorizar y bloquear, si los usuarios intentan salvar archivos con extensiones de música, video; en un volumen o recurso

- Podemos gestionar de reportes de almacenamiento como, por ejemplo; nivel de consumo de recursos, actividad relacionada con el screening de archivos y detección de patrones de uso.

Diseño General:

Figura N° 37: Creación de filtros de archivos.



Indicamos ruta de acceso al filtro de archivos, es decir, la carpeta o recurso al que se aplicará el filtro.
Si el filtro es **activo** significa que **no permitido**, **pasivo** es **si permitido**.
Definir propiedades personalizadas del filtro de archivos.
Creamos pues nuestro filtro para prohibir los ficheros de audio y video:

Figura N° 38: Definición de parámetros

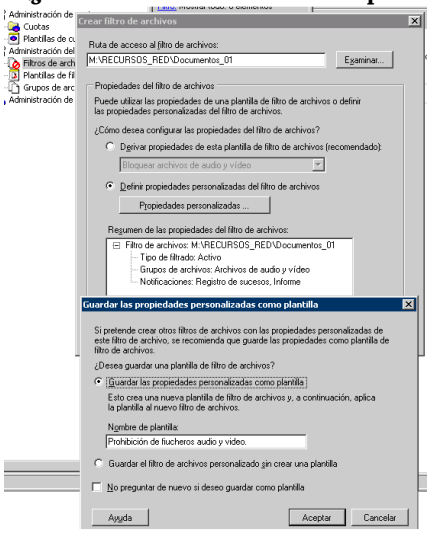


Figura N° 39: Filtro configurado.

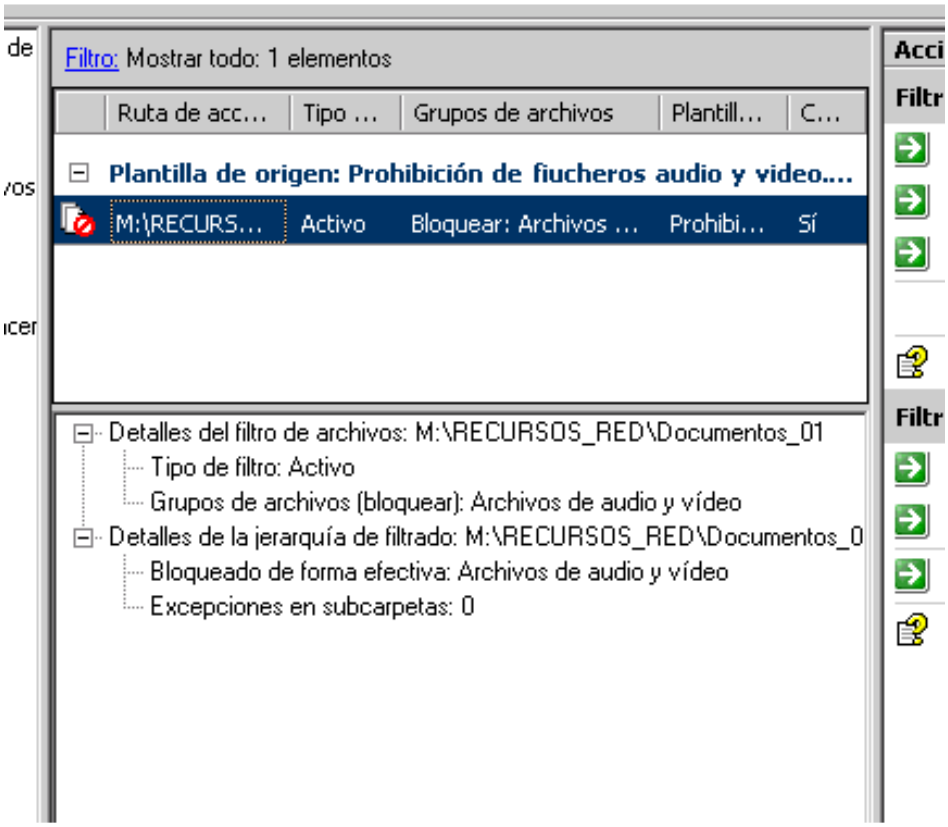


Figura N° 40: Intento de copiado de archivo audio en el recurso compartido:

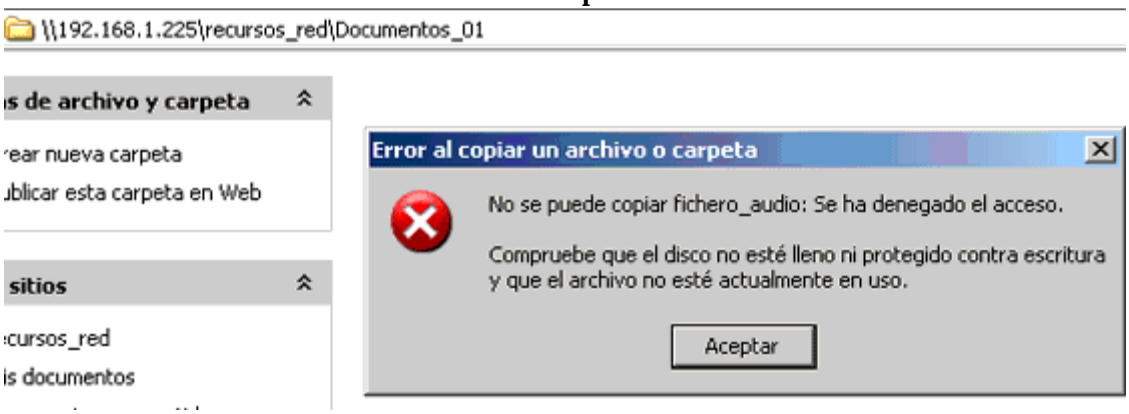
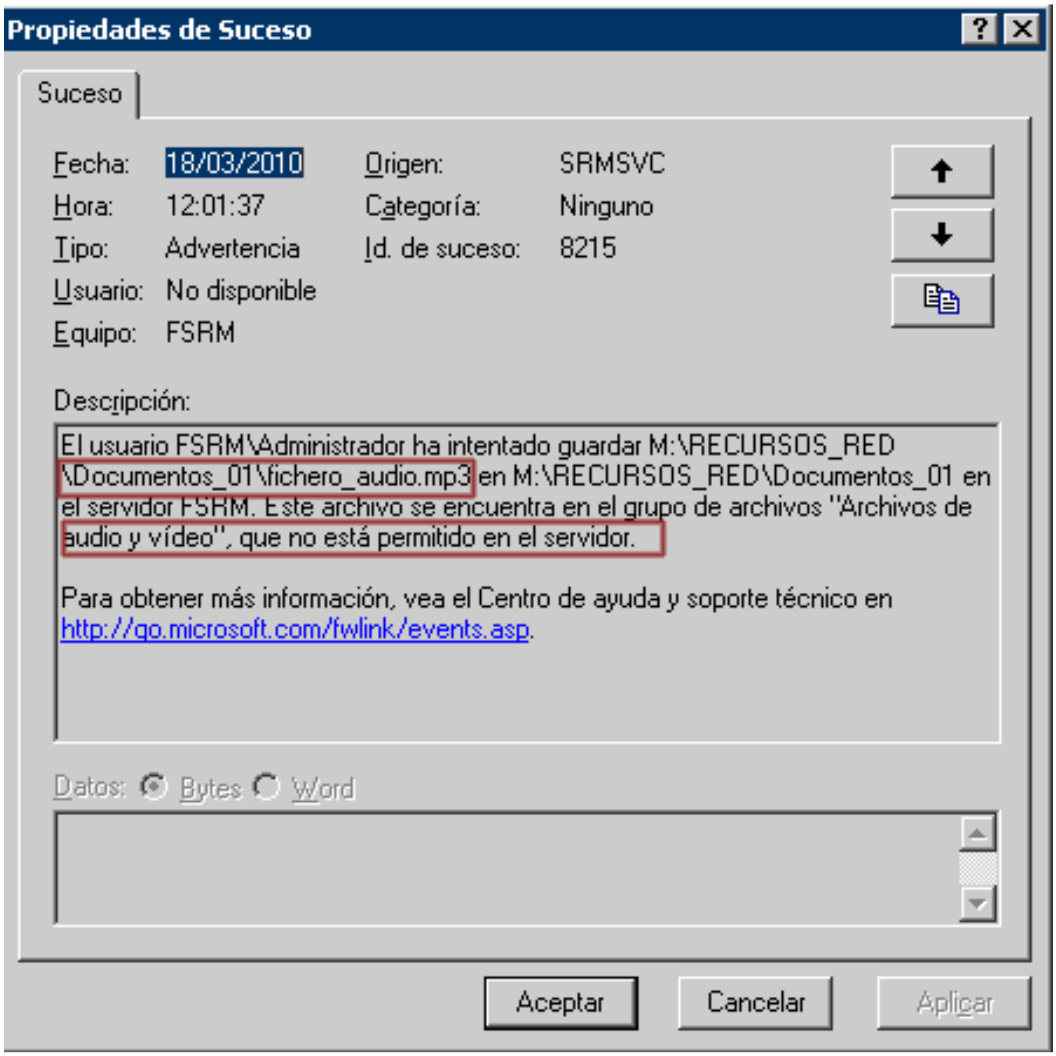


Figura N° 41: Generación de Suceso:

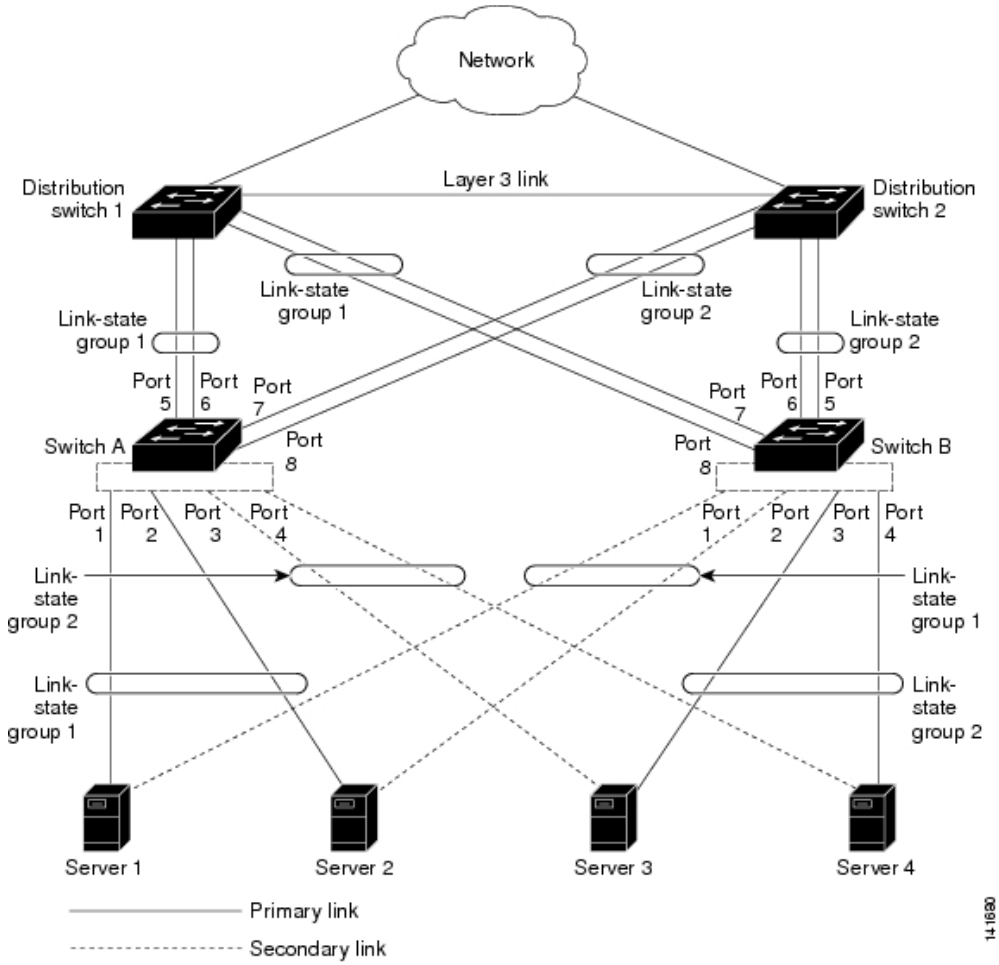


4.15. Implementación de Agregados de Enlace (LACP)

El uso de agregados de enlace, permitirá a los enlaces troncales administrar mejor el tráfico, brindándole un mejor rendimiento a la red.

En la siguiente imagen observamos los enlaces troncales interconectados entres los switches.

Figura N° 42. Diagrama implementación LACP



- Para poder realizar este agregado de enlace, debemos de configurar los puertos de nuestros switches e indicarles que los tales trabajaran como un solo enlace, adjuntando su velocidad.
- Por ejemplo, necesitamos que los 2 puertos GigabitEthernet del Switch, se establezcan como un solo enlace agregado al grupo 5 de EthernetChannel con el protocolo de control de Agregado de enlace (LACP)

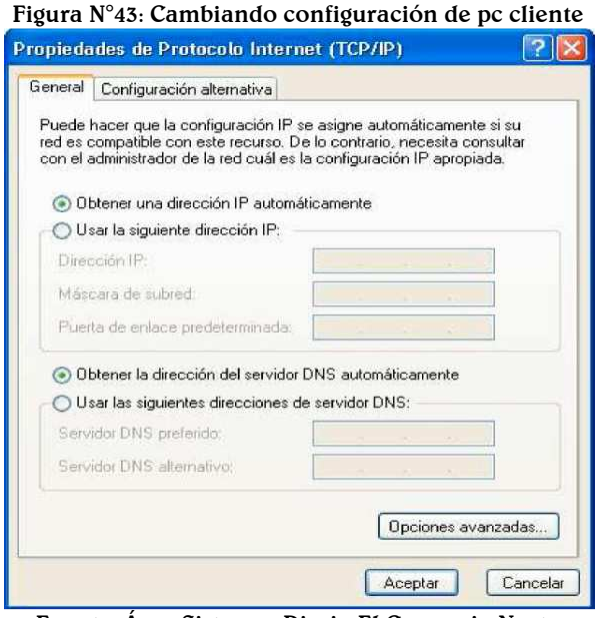
Configuración:

Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if)# channel-protocol lacp
Switch(config-if-range)# end

4.16. DHCP – Funcionalidad en Router Cisco 2800 Series.

DHCP o Dynamic Host Configuration Protocol, un protocolo que será instalado en el **Router Cisco 2800 Series** y que permitirá la configuración automática del protocolo TCP/IP de todos los clientes de dicha red. También nos permitirá obviar el tedioso trabajo de tener que configurar el protocolo TCP/IP cada vez que agregamos una nueva máquina a la red, por ejemplo, dirección IP, servidores DNS, gateway, WINS , etc.
Se podrá modificar la configuración de todos los equipos de la red con sólo modificar los datos del servidor.

Figura N°43: Cambiando configuración de pc cliente



Fuente: Área Sistemas Diario El Comercio Norte

- Después de configurar cambios en el Router Cisco 2800 Series, será necesario aplicar cambios en las propiedades de las tarjetas de red de cada dispositivo.

4.16.1. FASE IV. Documentar Implementación

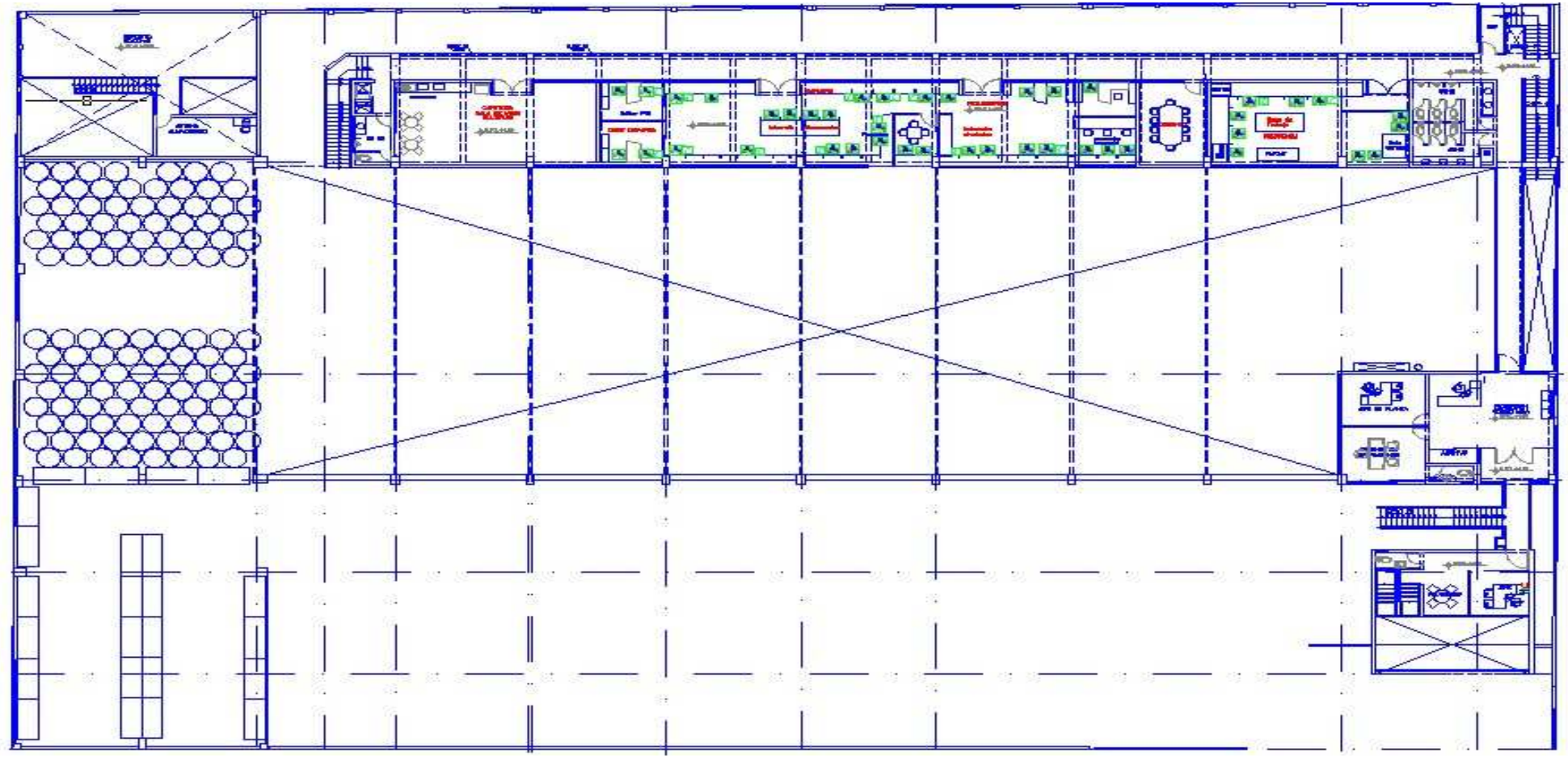
4.16.1.1. Plan de Implementación Física:

El simulador de Redes Cisco Packet Tracer 5.3, nos brinda la posibilidad de mostrar un diseño físico acorde a la realidad de nuestro proyecto.

En las siguientes imágenes mostramos lo dispositivos de red y los dispositivos finales organizado de acuerdo a las áreas de la Empresa editora el Comercio.

Plano N° 01: Diseño Físico Empresa Editora El Comercio Planta Norte

En el diseño físico de la empresa editora El Comercio Norte se detalla la forma de conectividad de los dispositivos de red.



A) Administración de Red - Sistemas

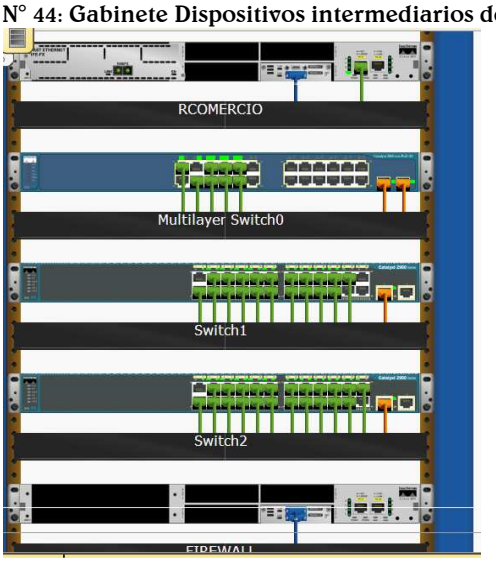
En esta área se encuentra la administración total de nuestra red corporativa, en la siguiente imagen mostramos el Rack con los dispositivos de red requeridos en nuestro diseño.
Comprende los siguientes dispositivos:

- **1 Router Cisco 2800 (Router principal- Nombre RComercio)**
- **1 Firewall Cisco ASA 5520**
- **1 Switch Cisco Catalyst 3560 (Función Core de la Lan)**
- **2 Switches Cisco Catalyst 3560(Cumplirán función de capa de Acceso)**

A su vez dentro de esta misma área se encuentran el conjunto de Servidores que soportan los procesos bajo distintos Sistemas que permiten que el Diario se produzca día a día tales como:

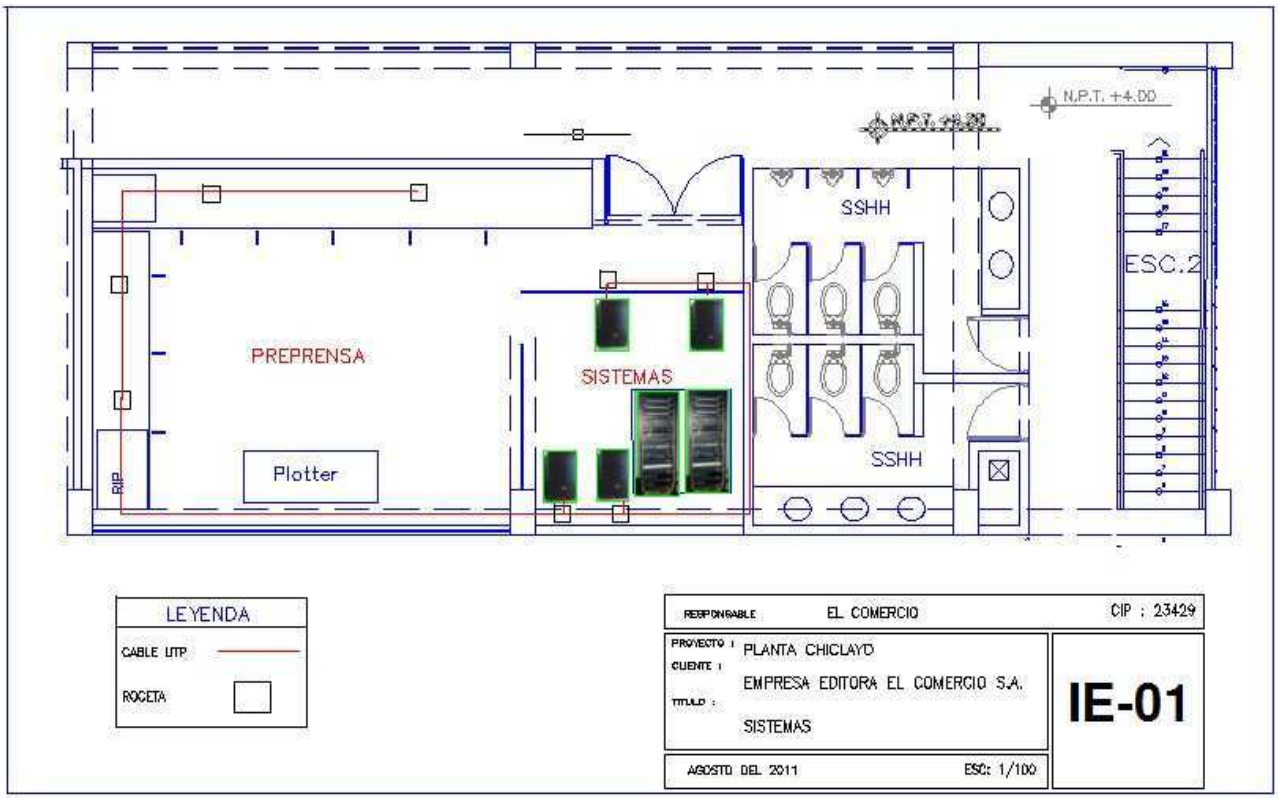
- **Servidor de DATOS:** Encargado de soportar y almacenar todos los distintos archivos de Fotos, Videos, Textos, etc. A su vez también aloja al aplicativo PrintPlotter Management.
- **Servidor NOVELL:** Soporta toda la información de la Promoción del Diario Trome "La llamada Ganadora".
- **Servidor SAP:** Soporta uno de los principales Sistemas de la empresa; Sistema SAP.
- **Servidor FTP:** Esta alojado en el **Servidor de Datos** – como propósito masivo de descarga de archivos enviados por las agencias de noticias.
- **Servidor ARKITEX:** Controla el proceso de autentificación y validación de los usuarios de la Lan, esta reforzado por un Servidor Radius. También alberga el aplicativo DTI, que es donde confluyen las páginas de los Diarios para su impresión. Asimismo soporta el programa Proxy Jana 2.4 que parametriza el acceso a determinadas páginas web. Actúa como **Controlador de Dominio**.

Figura N° 44: Gabinete Dispositivos intermediarios de Red



Fuente: Imagen proporcionada por Packet Tracert.

Plano N° 02: Distribución de Servidores Área Sistemas



B) Área Administración

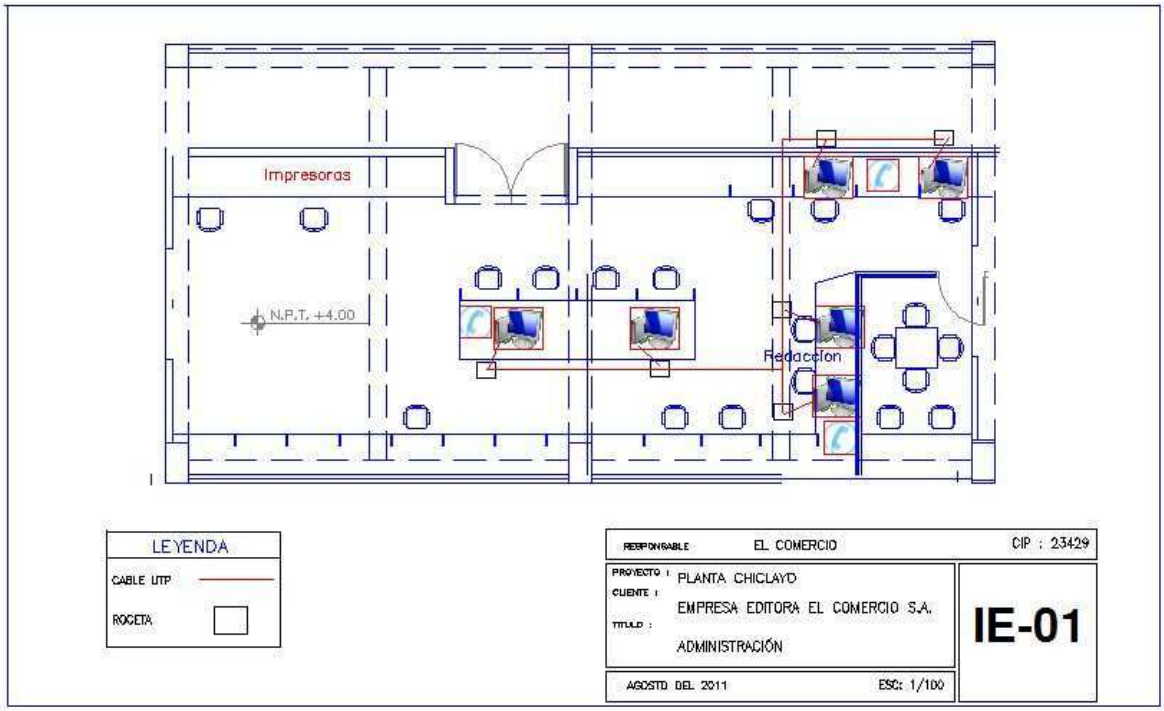
Esta área cuenta con los siguientes dispositivos:

- 8 computadoras personales
- 3 teléfonos IP Cisco 7942

Figura N° 45: Imagen de los terminales en el área de Administración

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 03: Distribución de PC's área de Administración



C) Seguridad

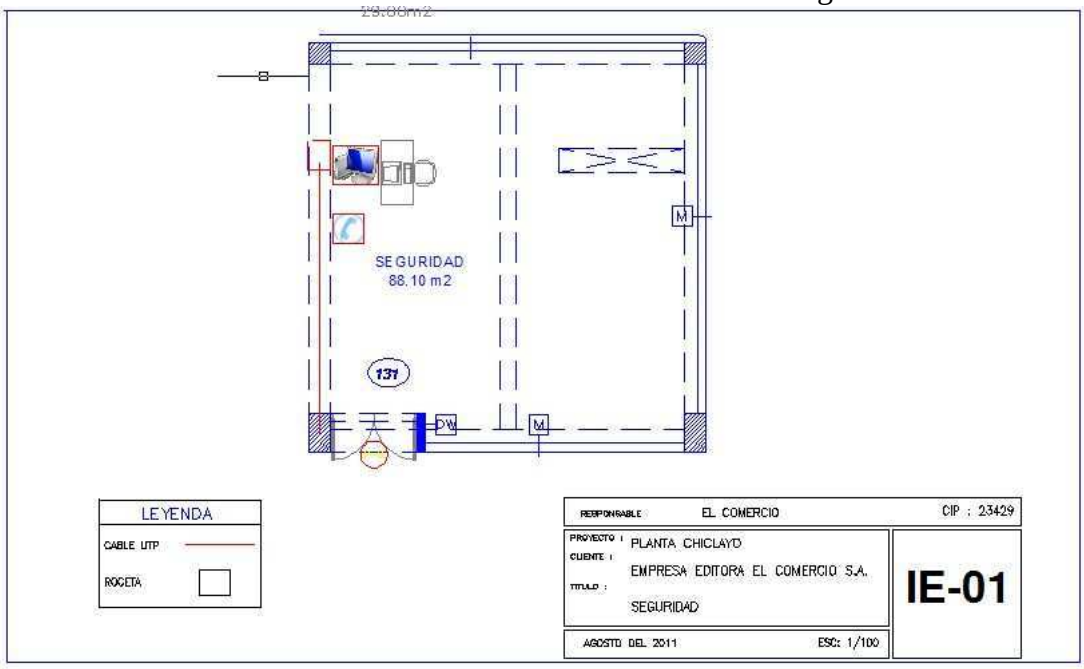
Esta área es la más pequeña y solo cuenta con los siguientes dispositivos:

- computadora personal
- Teléfono IP Cisco 7942

Figura N° 46: Imagen del terminal en el área de Seguridad

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 04: Distribución de terminales área Seguridad



D) Pre Prensa

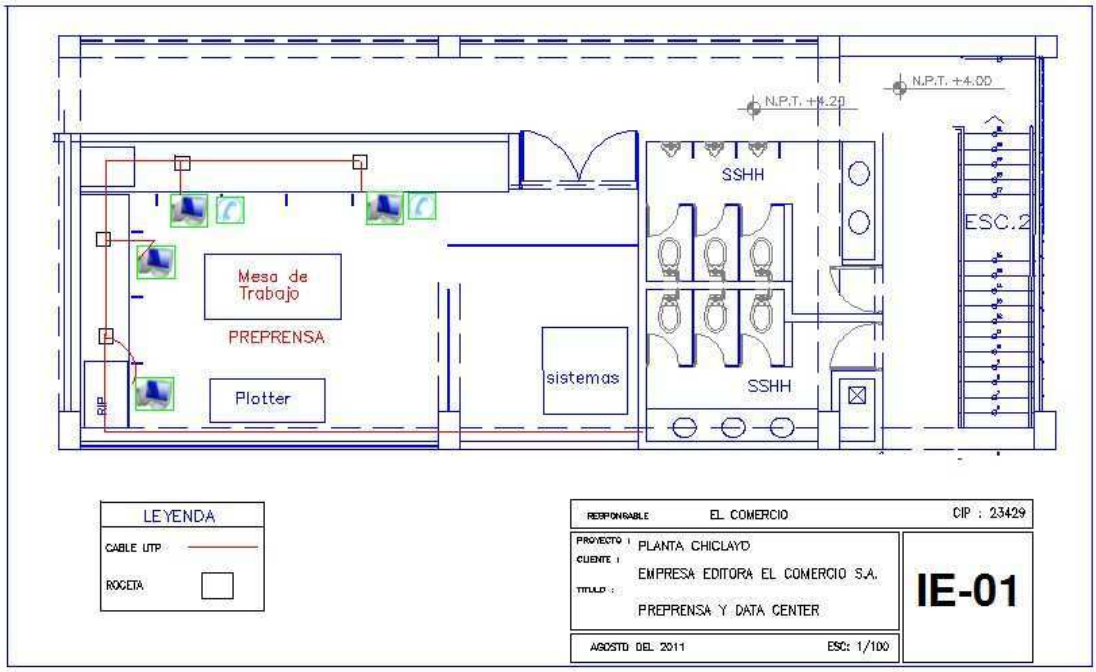
En esta área encontramos los siguientes dispositivos:

- 3 computadoras personales
- 2 teléfonos Ip Cisco 7942

Figura N° 47: Imagen de terminales en el área de Seguridad

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 05: Distribución de terminales área Preprensa



E) Redacción

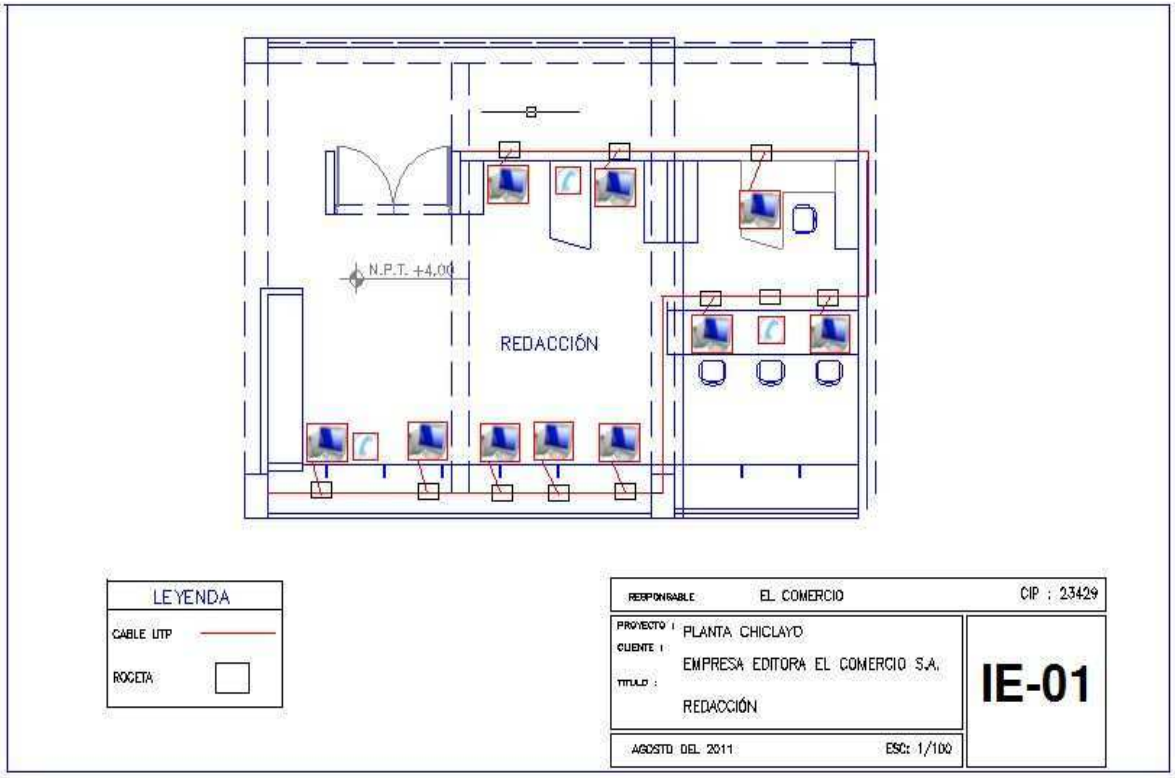
En esta área encontramos los siguientes dispositivos:

- 10 computadoras personales
- teléfonos IP Cisco 7942

Figura N° 48: Imagen de terminales en el área de Redacción

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 06: Distribución de terminales área Redacción



F) Publicidad

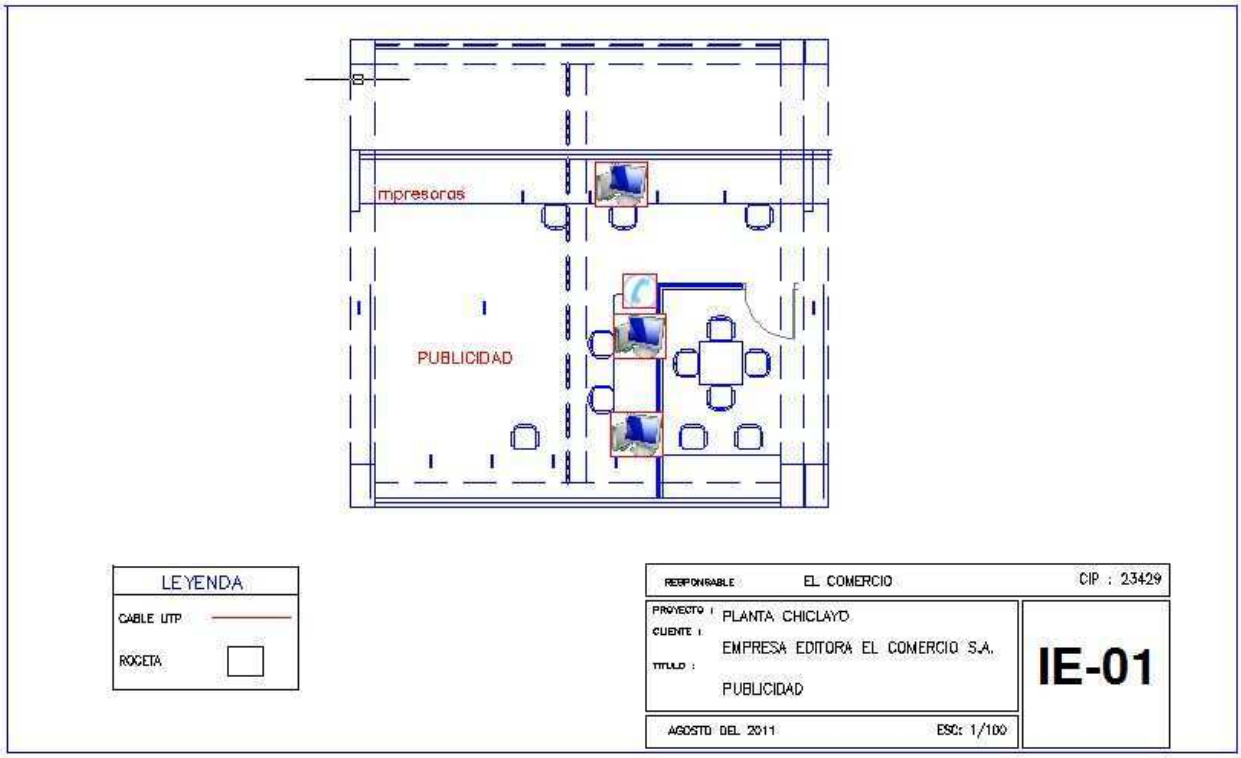
En esta área encontramos los siguientes dispositivos:

- 3 computadoras personales
- 1 teléfono Ip Cisco 7942

Figura N° 49: Imagen de terminales en el área de Publicidad

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 07: Distribución de terminales área Publicidad



G) Rotativa

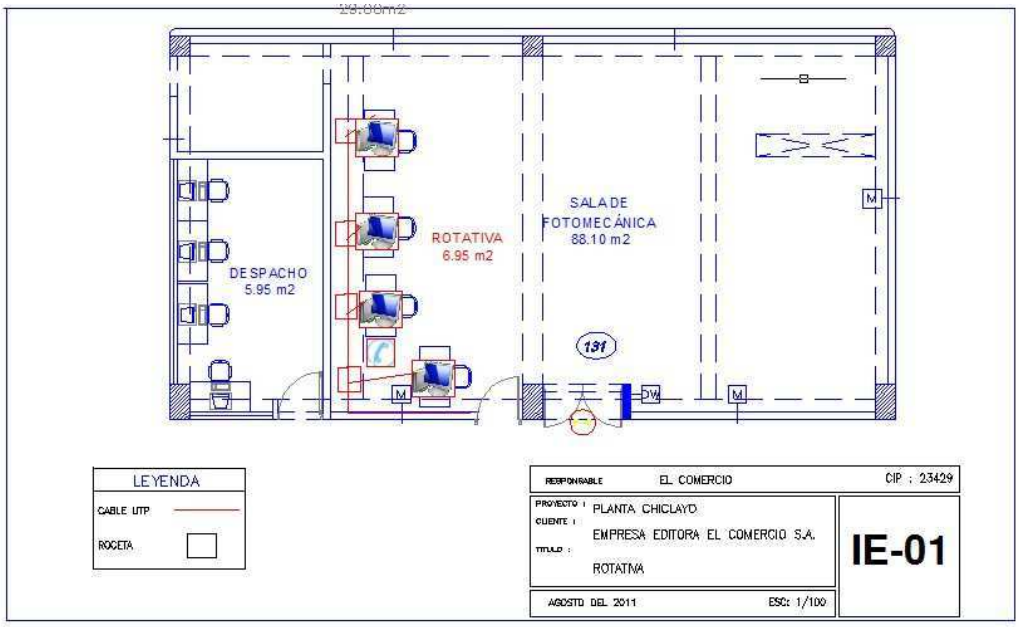
En esta área encontramos los siguientes dispositivos:

- 4 computadoras personales
- 1 teléfono Ip Cisco 7942

Figura N° 50: Imagen de terminales en el área de Rotativa

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 08 Distribución de terminales área Rotativa



H) Despacho

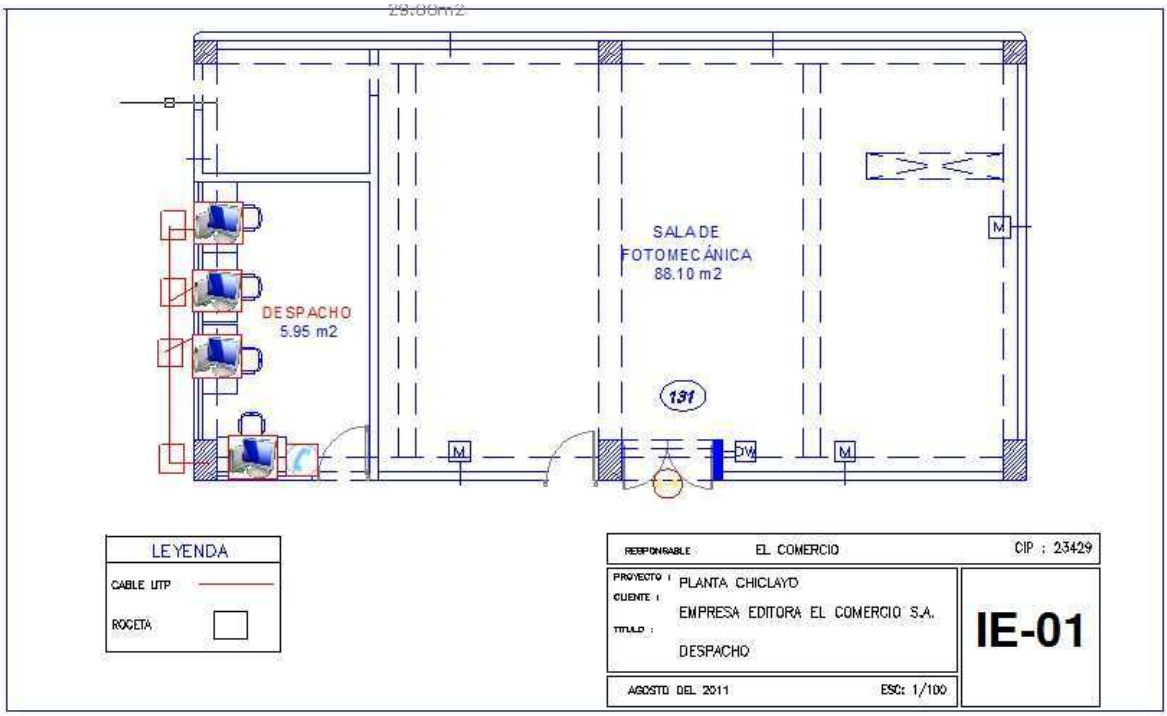
En esta área encontramos los siguientes dispositivos:

- 4 computadoras personales
- 1 teléfono Ip Cisco 7942

Figura N° 51: Imagen de terminales en el área de Despacho

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 09: Distribución de terminales área Despacho



I) Circulación

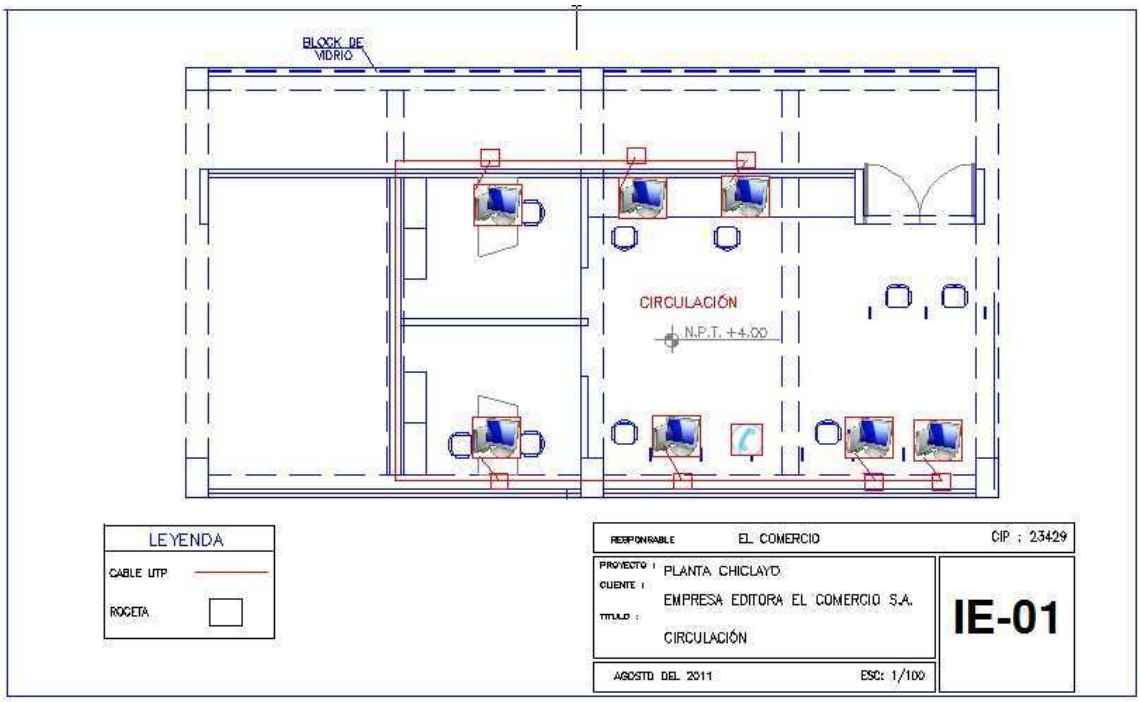
En esta área encontramos los siguientes dispositivos:

- 6 computadoras personales
- 1 teléfono Ip Cisco 7942

Figura N° 52: Imagen de terminales en el área de Circulación

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 10: Distribución de terminales área Circulación



J) Mantenimiento

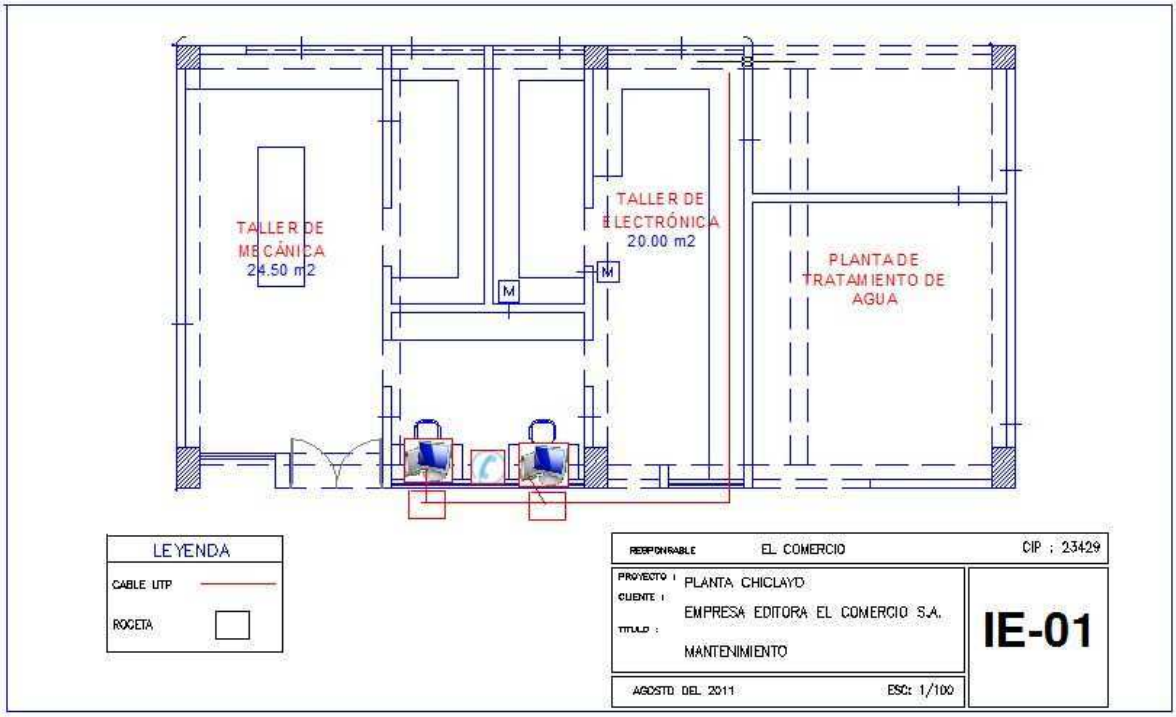
En esta área encontramos los siguientes dispositivos:

- 4 computadoras personales
- 1 teléfono Ip Cisco 7942

Figura N° 53: Imagen de terminales en el área de Mantenimiento

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 11: Distribución de terminales área Mantenimiento



K) Almacén

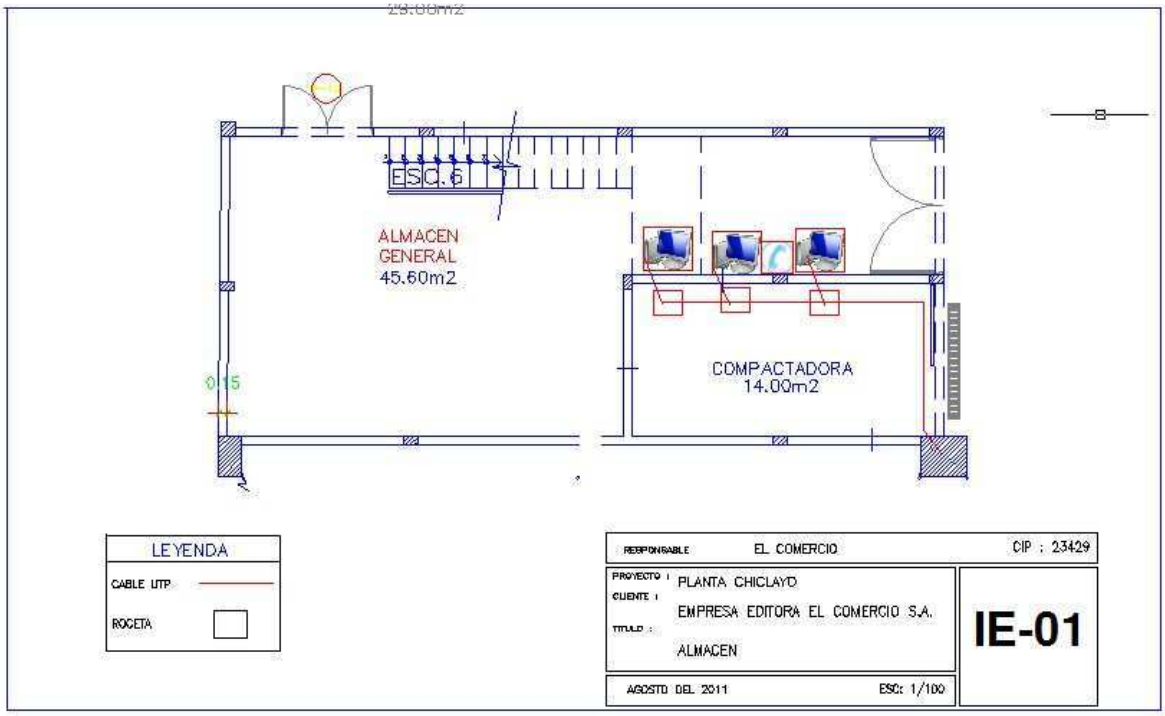
En esta área encontramos los siguientes dispositivos:

- computadoras personales
- teléfono Ip Cisco 7942

Figura N° 54: Imagen de terminales en el área de Almacén

Fuente: Imagen proporcionada por Packet Tracer.

Plano Nº 12: Distribución de terminales área Almacén

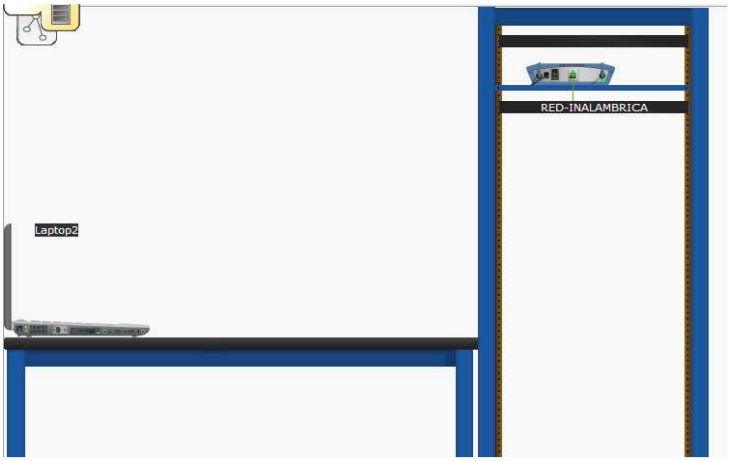


L) Invitado

En esta área encontramos los siguientes dispositivos:

- 1 Access Point LinkSys
- Computadoras portátiles de acuerdo a la cantidad de usuarios visitantes.

Figura N° 55: Imagen de terminales en el área de Almacén

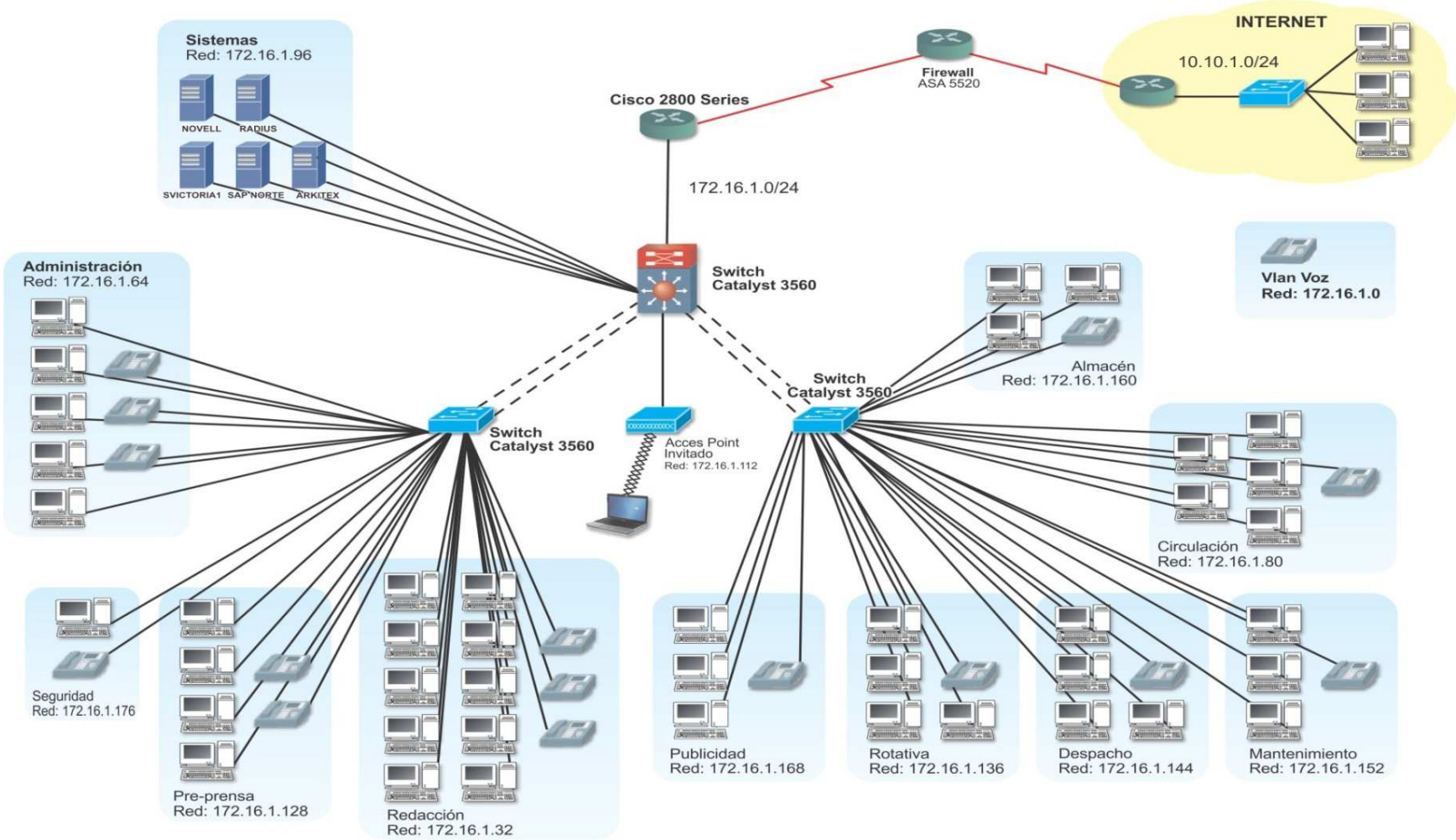


Fuente: Imagen proporcionada por Packet Tracer.

M) Plan de Implementación Lógica:

Figura N° 56: Diseño Lógico propuesto.

En el diseño lógico de Chiclayo se detalla el direccionamiento IP de las VLAN's de cada área.



N) Costos de Implementación

- En lo que refiere a equipos, se implementó las soluciones sobre la plataforma física instalada como son los equipos de la familia Cisco : Router 2800 Series (Cant. 1) y Switches 3560 POE (Cant.3), cuyo valor no se considera en el costo.

4.16.2. Costos Mano de Obra.

El costo en que se incurre es básicamente de Configuración.

Actividades	Número de Trabajadores	Total Costo s/.
Configuración Tecnologías de seguridad	2	500
Configuración de VLAN´s	2	1000.00
Configuración de Servidor AAA RADIUS	2	500.00
Configuración de QoS	2	500.00
Configuración de Agregados de Enlace - FTP	2	1000.00
S/. 3500.00		

Cuadro Nº 14: Costos mano de obra

4.16.3. Características de los equipos para implementar la solución:

- **Cisco 2800 Routers de Servicios Integrados**

  Los Routers de Servicio Integrado (ISRs) de Cisco 2800 son de una serie galardonado entendida para empresas pequeñas a medianas y oficinas Enterprise. Routers Cisco 2800 han sido creado para entrega wire-speed de servicios simultáneos de seguridad alta y tiene cabida para conexiones T1/E1 para servicios incluyendo datos, seguridad, voz, video y inalámbrico.

Cuadro Nº 15: Características de Serie Cisco 2800 General:

General	
Tipo de dispositivo	**Encaminador**
Factor de forma	**Externo - modular - 1U**
Anchura	**43.8 cm**
Profundidad	**41.7 cm**
Altura	**4.5 cm**
Peso	**6.4 kg**
Memoria	
Memoria RAM	**256 MB (instalados) / 768 MB (máx.) - DDR SDRAM**
Memoria Flash	**64 MB (instalados) / 256 MB (máx.)**
Conexión de redes	

Tecnología de conectividad	**Cableado**
Protocolo de interconexión de datos	**Ethernet, Fast Ethernet**
Red / Protocolo de transporte	**IPSec**
Protocolo de gestión remota	**SNMP 3**
Indicadores de estado	**Actividad de enlace, alimentación**
Características	**Diseño modular, protección firewall, cifrado del hardware, asistencia técnica VPN, soporte de MPLS, Quality of Service (QoS)**
Cumplimiento de normas	**IEEE 802.3af**
Expansión / Conectividad	
Total ranuras de expansión (libres)	**4 (4) x HWIC 1 (1) x NME 2 (2) x AIM 2 (2) x PVDM - SIMM 80-PIN 2 memoria 1 Tarjeta CompactFlash**
Interfaces	**2 x USB 2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 1 x gestión - consola - RJ-45 1 x serial - auxiliar - RJ-45**
Diverso	
Algoritmo de cifrado	**DES, Triple DES, SSL 3.0, AES de 128 bits, AES de 192 bits, AES de 256 bits**
Método de autentificación	**Secure Shell v.2 (SSH2)**
Cumplimiento de normas	**CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2**
Alimentación	
Dispositivo de alimentación	**Fuente de alimentación – interna**
Voltaje necesario	**CA 120/230 V (50/60 Hz)**
Software / Requisitos del sistema	
Software incluido	**Cisco IOS IP Base**
Parámetros de entorno	
Temperatura mínima de funcionamiento	**0 °C**
Temperatura máxima de funcionamiento	**40 °C**
Ámbito de humedad de funcionamiento	**5 - 95%**

- SWITCH CISCO 3560

Características

Descripción del producto Cisco Catalyst 3560-P0E - conmutador - 48 puertos

Cuadro Nº 16: Switch Cisco 3560

Tipo de dispositivo	**Conmutador**
Factor de forma Externo	- 1U
Dimensiones	44.5 cm x 37.8 cm x 4.4 cm
Peso	6.1 kg
Memoria RAM	128 MB

Memoria Flash	32 MB
Cantidad de puertos	48 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Ranuras vacías	4 x SFP (mini-GBIC)
Protocolo de gestión remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, SSH-2
Modo comunicación	Semidúplex, dúplex pleno
Características	Capacidad dúplex, conmutación Layer 3, conmutación Layer 2, auto-sensor por dispositivo, Encaminamiento IP, soporte de DHCP, alimentación mediante Ethernet (PoE), negociación automática, concentración de enlaces, soporte de MPLS, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico, activable, snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), Servidor DHCP, Virtual Route Forwarding-Lite (VRF-Lite), rastreador MLD, Dynamic ARP Inspection (DAI), Time Domain Reflectometry (TDR)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s
Alimentación por Ethernet (PoE)	Si
Alimentación	CA 120/230 V (50/60 Hz)

V. DISCUSIÓN

El desarrollo presentado nos permite verificar la hipótesis planteada sobre la mejora del rendimiento y seguridad de la RED

Cuadro Nº 17: Contrastación de Hipótesis:

INDICADOR	ITEM	PRETEST	POSTTEST	DIFERENCIA	BROADCAST
Velocidad o tasa de transferencia de datos	Ancho de Banda disponible en Horas pico	3 Mbps	8.5 Mbps	5 Mbps	
	Porcentaje de buen rendimiento de la Red	30 %	85 %	55%	
Disponibilidad de Servicios	Disponibilidad continua 24 horas x 7 días	No	Sí		
	Frecuencia de interrupciones	3/Día	0		
Latencia de Red	Tipos de paquetes identificados para priorización del Ancho de Banda	0	3 (Datos, VoIP, Video)		
	Tiempo en la ejecución de procesos de alta prioridad	5 horas	3.5 horas	1.5 horas	
	Tiempo para transferencia de videos e imágenes	50 min.	8 min.	42 min.	
Accesos a Recursos compartidos	Segmentos de Red de acuerdo a afinidad de usuarios o áreas	1	15		
Control o Filtros de paquetes externos e internos	Listas Control de Acceso implementadas	0	5		
Autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario.	Mecanismos de autenticación implementados	1	3 (RADIUS y Active Directory, Acl)		
Cantidad de Dominios Broadcast.	Mecanismo de segmentación y reducción de la propagación de Dominios de Broadcast	1	16	15	Mitigacion de tormentas de broadcast al impedir que se propague por la red deliberadamente

- Que la velocidad o tasa de transferencia de datos en horas pico denotaba 3 Mbps frente a 8.5 Mbps como indicador actual de la red. Es decir que el ancho de banda disponible en horas críticas no era suficiente para soportar el flujo masivo de información en tiempo real (400 Mbps) por lo que la implementación de estrategias QoS ha permitido la mejora sustancial de la velocidad en la red LAN.

- Las interrupciones o cortes de conexión fueron mermadas en un 85% gracias a los mecanismos Balanceo de tráfico(LACP) , identificación de paquetes, y por ende, su categorización en el uso de ancho de banda; estrategia que logró reducir el tiempo de los procesos Core del negocio en 90 minutos, tiempo que abre una brecha para los procesos de impresión, distribución y circulación de los diarios el cual representa un manejo externo del producto final pero que sin embargo se ven directamente beneficiados tanto en costos productivos, operativos y económicos.

- El acceso a los servicio y recursos compartidos de la red se han visto reforzados como consecuencia de la configuración de tecnologías de seguridad emergentes, propias de la versión de los controladores de dominio actual (Windows Server 2008), detalles que no aplican tesis anteriores como propuesta de solución para aplicar controles ante los riesgos de seguridad. Estos nuevos mecanismos han permitido elevar el nivel de seguridad en un 95% mejoras que satisfacen las exigencias y lineamientos estratégicos de la empresa. Asimismo estas mejoras se ven reforzadas por el uso de un Firewall ASA 5550, el cual trabaja en concordancia con el Servidor Radius, logrando un nivel de seguridad superior.

- La nueva estructura lógica de la Red, predispone una estructura física más robusta permitiendo la escalabilidad de la LAN la cual permite soportar un crecimiento tecnológico.

VI. CONCLUSIONES

a) La proyección de crecimiento de la Planta Norte es de 16% anual, donde actualmente se cuenta con 50 terminales. Se implementó y configuró la red para soportar este promedio de crecimiento sin afectar el rendimiento de la Lan, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch Cisco de 48 puertos hacia el swicth Core y responder a la tasa de crecimiento, con una velocidad de 100/1000 Gbps en cada troncal. Con ello concluimos que el objetivo de la Escalabilidad fue posible.

b) La velocidad o tasa de transferencia de datos está operando dentro de los rangos esperados, gracias a la implementación de técnicas de balanceo y priorización de trafico con QoS, el cual se configuró en los dispositivos que consumen mayor ancho de banda (Teléfonos IP, Pc's periodistas y Preprensa),identificándose tipos de paquetes (Voz, Datos y Video) para reservar un ancho de banda de origen a destino donde los equipos detectan el tráfico de datos relevantes y lo gestionan con mayor prioridad (Video y Voz). Asimismo se implementó mejoras físicas para reforzar la implementación lógica, como es el uso de LACP (Enlaces agregados) entre los switch principales y secundarios, multiplicando el ancho de banda en una proporción de 1 a 4, logrando de esta manera cumplir con el objetivo deseado.

c) La configuración de un Firewall Cisco - físico, VLAN's, ACL's, DHCP en el Router, el uso de aplicativos emergentes propios del Windows Server 2008 (File Screening Management, NetWork-Access Protection) ha propiciado la solución a la problemática de la perdida de información compartida en red, ofreciendo una administración de recursos más controlada y eficiente, mejorando al mismo tiempo la seguridad de la Red.

d) El protocolo VTP (Virtual Trunking Protocol) es de gran ayuda para no tener que configurar las VLANs en todos los switches, simplemente se debe configurar las VLANs en el switch que esté en modo servidor, y el resto de switches debe estar en modo cliente.

e) El tráfico de voz también se optimiza debido a la configuración de priorización en el trafico con el estándar IEEE 802.1p, lo cual indica a los switches jerarquizar la transmisión de la data mediante la gestión de las colas de estas tramas.

f) Se ha Implementado mecanismos para autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario, como RADIUS que trabaja con Active Directory, lográndose un mejor nivel de seguridad, dado que los filtros son más rigurosos gracias a las capas de seguridad que brinda Radius. Asimismo se modificaron privilegios de usuarios en el Active Directory, para estar alineados al nuevo esquema de trabajo en red y uso de recursos.

VII. RECOMENDACIONES

a) Establecer como política de administración, que solo las personas que administran y dan mantenimiento a la red tengan acceso a los equipos de interconexión de red, especialmente para la tarea más cotidiana que es el ingreso, salida o cambio de hosts, para que éste personal con el conocimiento claro de la distribución de VLANs, configure adecuadamente los puertos de los switches.

b) Configurar e implementar tecnología LACP (Agregados de Enlace) a nivel de Servidores – Switch, para mantener un esquema similar entre dispositivos intermedios. Logrando así ofrecer una mayor eficiencia en el balanceo y tráfico de carga de datos.

c) Implementar acciones de revisión física de la red, descartando equipos conectados sin autorización. Asimismo implementar políticas de conexión para equipos invitados o externos.

d) Instalar Access Point en distintos puntos de la Planta para una mayor cobertura y conectividad, mejorando así el acceso a los recursos de la red a los usuarios que necesitan estar trasladándose dentro de las instalaciones.

VIII. REFERENCIAS BIBLIOGRÁFICAS.

Material impreso.

- ✓ CISCO. Networkers Solutions Forum Routed Fast Converence and High Availability, 2006.
- ✓ COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. México: Prentice–Hall, 1996.
- ✓ REGIS, Joseph. Comunicaciones Inalámbricas de Banda Ancha. McGraw-Hill, 2003.
- ✓ STALLINGS, William. Comunicación y redes de computadoras. Pearson-Education, 2000.
- ✓ STALLINGS, William. Organización y arquitectura de computadoras. Great Prentice-Hall, 2006.
- ✓ STALLINGS, William. Redes de internet de alta velocidad. Pearson-Educación, 2003.
- ✓ TANENBAUM, Andrew. Redes de Computadoras. México: Prentice – Hall, 2003.

Recursos bibliográficos en línea.

- ✓ "Redes Virtuales VLANs." (2011 [citado el 16 de Marzo de 2011]) disponible en http://www.textoscientificos.com/redes/redes-virtuales
- ✓ Calle, Ingrid. "Configuración: Tecnología DSL." (2007 [citado el 25 de Junio de 2011]) disponible en http://www.uninorte.edu.co/divisiones/ingenierias/Dpto_Sistemas/lab_redes/upload/file/Configuracion_de_Tecnologia_%20ADSL.pdf
- ✓ Castañeda, Luis. "Simuladores de Redes Cisco." (2010 [citado el 23 de Junio de 2011]) disponible en http://www.slideshare.net/aaron12/simuladores-de-redes-cisco
- ✓ Della, Jorge."Modelo de Referencia OSI." (2005 [citado el 28 de Abril del 2011]) editado por Mario Navarro: disponible en http://www.frm.utn.edu.ar/comunicaciones/modelo_osi.html
- ✓ http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf
- ✓ http://www.redescisco.net/archivos/clases_online/Clase1_ACL.pdf

- ✓ http://www.redescisco.net/v2/art/la-encapsulacion-de-datos-un-concepto-critico/

- ✓ Medina, Luis. "Diseño de Redes, Modelo Jerárquico." (2011 [citado el 06 de Junio de 2011]) disponible en http://www.redesymas.org/2011/05/diseno-de-redes-modelo-jerarquico.html

- ✓ Millán, Ramón. "La tecnología de acceso ADSL." (1999 [citado el 24 de Junio de 2011]) disponible en http://www.ramonmillan.com/tutoriales/adsl.php

- ✓ Redes CISCO. "La encapsulación de datos, un concepto crítico." (2010 [citado el 29 de Abril de 2011]) editado por Paulo Colomés: disponible en

- ✓ Romero, María. "Calidad de servicios QoS en redes." (2010 [citado el 21 de Junio de 2011]) disponible en

- ✓ Spichiger, Juan Carlos. "Listas de control de acceso·" (2010 [citado el 27 de Mayo del 2011]) disponible en

- ✓ TICOM. "como usar ftp paso a paso." (2010 [citado el 16 de Julio de 2011]) disponible en http://www.ticomperu.com/manualdeftppasoapaso.htm

IX. ANEXOS

ANEXO I:

Cuadro Nº 18: Evolución del crecimiento en Hardware

Año	Nro. Equipos	Crecimiento respecto del año anterior (%)
2006	23	--
2007	28	22%
2008	35	25%
2009	40	14%
2010	45	12%
2011	51	11%

%Promedio Crecimiento Anual = 16%

ANEXO II:

Medición del Rendimiento de la Red.

Dimensionamiento del Tráfico

Para realizar el dimensionamiento del tráfico que circula por la red, se hizo un análisis estadístico del uso de las aplicaciones que se ejecutan en la Planta Norte - Chiclayo, debido a que no existen antecedentes de comportamiento de la red desde los puntos locales y remotos hacia el servidor principal.

Velocidad efectiva promedio de las aplicaciones de la red

La velocidad efectiva es la velocidad de transmisión instantánea generada por una aplicación en la red, el mismo que permitirá dimensionar el tráfico. Para las siguientes aplicaciones se tiene:

Utilización de instrumentos medición de los flujos de la Red

a. Análisis con Software PTRG Network Monitor

- **Correo electrónico**

  La información que se intercambia por *e-mail* corresponde principalmente a informes, gráficos estadísticos, videos, notas periodísticas e información general.

  Debido a que un documento de texto tiene aproximadamente un tamaño de 2 Mbytes en tanto que un documento gráfico posee un mayor tamaño, de acuerdo al formato de la imagen que se desee transmitir teniendo un promedio de 8 Mbytes, se considera que el tamaño promedio de los archivos que se envían, redondeando, es de 5 Mbytes.

  Para el acceso de correo electrónico, se ha estimado que se revisa un promedio de 50 *e-mail's* en una hora y que existe un 60% de simultaneidad entre los 65 usuarios.

  Por lo tanto la velocidad efectiva que se maneja para correo electrónico para todos los usuarios es de:

$$V_{CO} = \frac{5000\,Kbytes}{correo} * \frac{8bits}{1byte} * \frac{50correos}{1hora * 1usuario} * \frac{1hora}{3600seg} * 65usuarios * 60\% = 21666.7kbps$$

- **Acceso a Internet**

  En este caso se ha considerado que una página Web tiene un peso aproximado de 100Kbytes, incluyendo texto e imágenes. Además, se ha estimado el número de páginas que un usuario accedería en una hora.

Por lo tanto se tiene:

$$V_{AI} = \frac{100\,Kbytes}{pagina} * \frac{8bits}{1byte} * \frac{30\,página}{1hora * 1usuario} * \frac{1hora}{3600\,s} * 65usuarios * 80\% = 346.67\,kbps$$

- **Tráfico para correo electrónico**

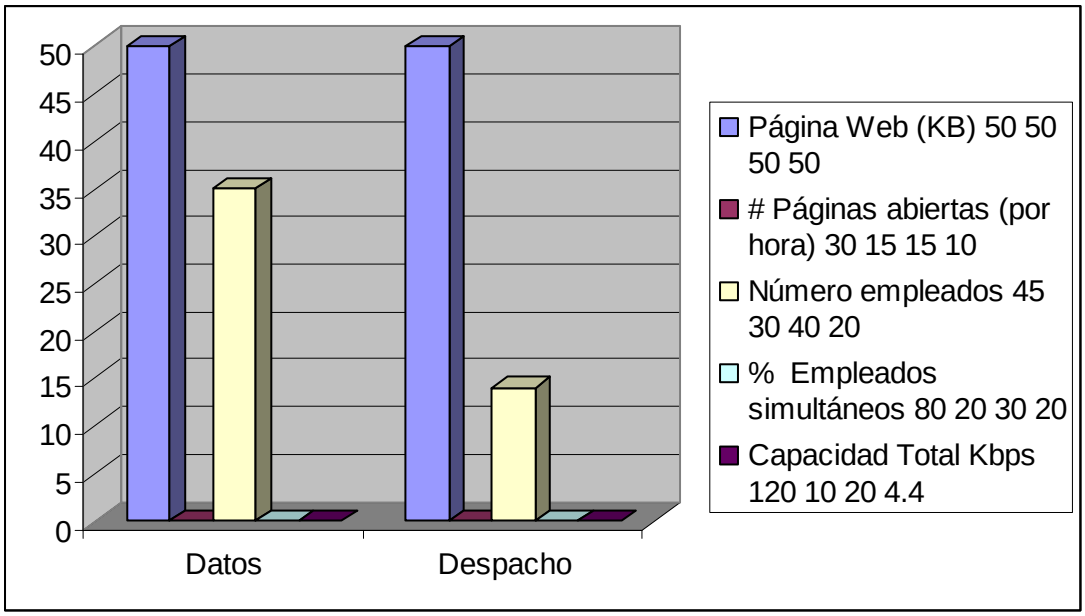
Departamento	Mail (KB)	# mail leídos por usuario (por hora)	Número empleados	% Empleados simultáneos abriendo mails	Capacidad Total Kbps
Jefatura Planta	1000	5	2	60	150
Prensa	1000	25	30	40	2500
Administración	1000	5	4	20	300
Publicidad	1000	5	3	15	50
Sistemas	1000	5	2	0	0
Despacho	1000	5	4	0	0
Total					3000

Cuadro N° 19: Tráfico para correo electrónico

- **Tráfico para páginas web**

Cuadro N° 20: Tráfico para páginas web

Departamento	Página Web (KB)	# Páginas abiertas (por hora)	Número empleados	% Empleados simultáneos abriendo Págs.	Capacidad Total Kbps
Jefatura Planta	50	30	2	80	120
Prensa	50	15	30	20	10
Administración	50	15	7	30	20
Publicidad	50	10	20	20	4.4
Sistemas	50	0	2	0	0
Despacho	50	0	14	0	0
Total					154.4


50
45
40
35
30
25
20
15
10
5
0
Datos
Despacho
Página Web (KB) 50 50 50 50
Páginas abiertas (por hora) 30 15 15 10
Número empleados 45 30 40 20
% Empleados simultáneos 80 20 30 20
Capacidad Total Kbps 120 10 20 4.4

- **Tráfico servidor datos**

Cuadro Nº 21: Tráfico servidor datos

Departamento	Datos (KB)	Consultas accedidas (por hora)	Número empleados	% Empleados simultáneos haciendo consultas	Capacidad Total Kbps
Jefatura Planta	2048	10	2	20	409.6
Prensa	2048	5	30	10	5000
Administración	2048	5	7	5	3000
Ventas	2048	20	4	30	546.13
Sistemas	2048	20	2	30	955.73
Despacho	2048	5	14	10	900
Total					10818.46

- **Tráfico plotter**

  Dado que existen 2 plotters para el departamento de Sistemas, el porcentaje de simultaneidad es de $\frac{2}{15} * 100 = 13.33\%$, aproximadamente 14%

Departamento	*Tamaño Archivo Imprimir (KB)*	*Impresiones (por hora)*	*Número Usuarios*	*% Impresiones Simultáneas*	*Capacidad Total Kbps*
Sistemas	10 000	50	15	14	25 000

- **Tráfico impresora**

  Dado que existe una impresora para el departamento de Sistemas, el porcentaje de simultaneidad es de $\frac{1}{15} * 100 = 6.67\%$, aproximadamente 7%

Departamento	Tamaño Archivo Imprimir KB	Impresiones (por hora)	Número empleados	% Impresiones Simultáneas	Capacidad Total Kbps
Sistemas	1000	50	15	7	11.66

- **Tráfico por departamentos (kbps)**

Departamento	Mail Kbps	Páginas Web	Base Datos	Servidor Local	Plotters	Impresora	Total
Jefatura Planta	300	120	409.6	0	0	0	829.6
PrePrensa	53.3	10	68.26	533.33	250	11.66	926.55
Administración	53.3	20	45.5	0	0	0	118.8
Publicidad	20	4.4	546.13	0	0	0	570.53
Sistemas	0	0	955.73	0	0	0	955.73
Despacho	0	0	31.85	477.86	0	0	509.71

Cuadro Nº 22: Tráfico por departamentos (kbps)

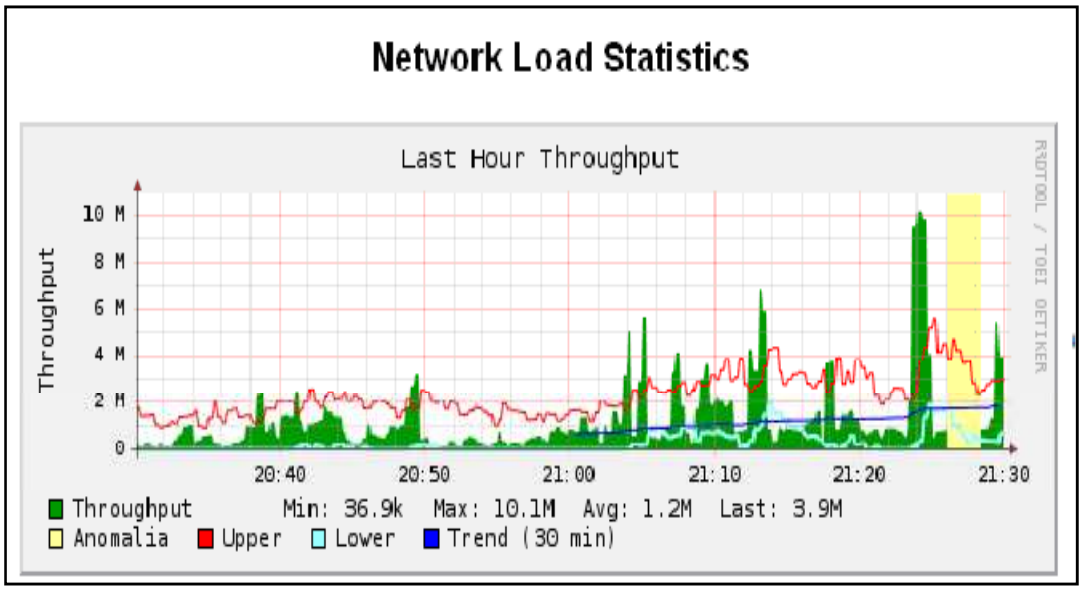
Como conclusión se tiene que en cada departamento supera el 1Mbps para el tráfico dentro de la red.

Los problemas mencionados anteriormente están presentes en la empresa Editora El Comercio – Planta Norte, un ejemplo de ello es el tráfico **LAN** que se tiene en la red de esta empresa, el trafico Lan es la cantidad de información que se envía / recibe dentro de una red local. La medición del tráfico de datos permitirá conocer el estado y funcionamiento general de la red.

El software PTRG Network Monitor fue instalado en el servidor de la red LAN, se activó todos los días hábiles desde las 7:30 am hasta las 11:30 pm, durante 4 semanas consecutivas correspondientes al mes de abril del 2011. La tabla Nº01 contienen información detallada de la medición en tiempo real del tráfico de la red tales como: Total de bytes enviados y recibidos, Promedio de carga de la Red, Pico en la carga de la Red, y Total de datos transmitidos.

Toda esta información se presenta en forma detallada y simple, a fin de facilitar su compresión. En la gráfica Nº01 podemos ver una de las tantas interfaces de este software.

Vista de la interfaz de Network Activity



Fuente: captura de pantalla del software

En la Tabla N°01 se han tabulado los datos correspondientes de la carga y picos de la red usando el mencionado software.

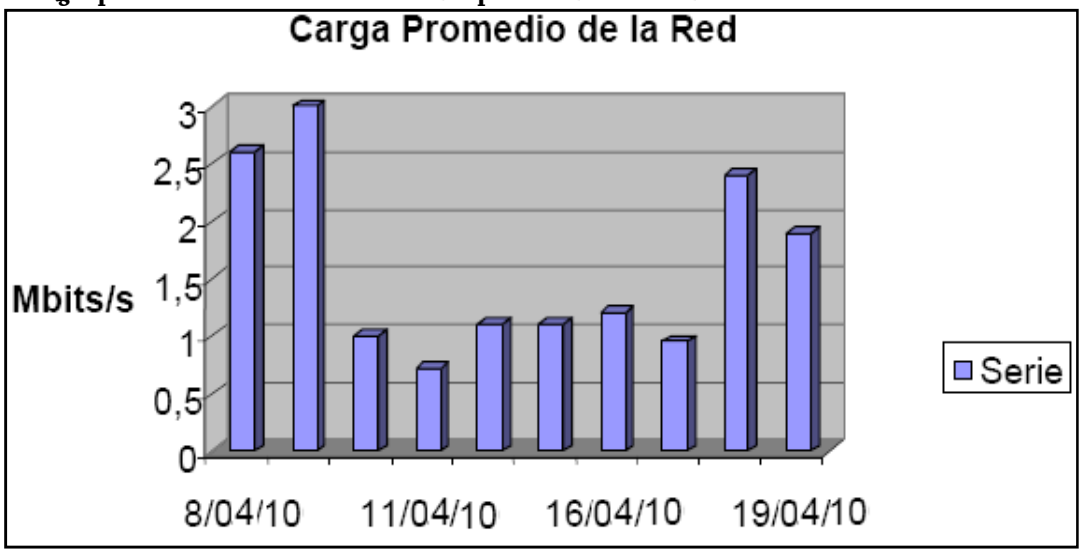
Tabla N°01 Datos de red LAN de la Empresa Editora El Comercio – Planta Norte.

	PROMEDIO DE CARGA DE RED		PICO EN LA CARGA DE RED	
Fecha	**Bits**	**Paquetes**	**Bits**	**Paquetes**
08/04/2011	2,6 Mbits/s	422.4 pkt/s	28,6 Mbits/s	4939.2 pkt/s
09/04/2011	3 Mbits/s	492.8 pkt/s	40,2 Mbits/s	5498.4 pkt/s
10/04/2011	1 Mbits/s	240 pkt/s	8 Mbits/s	1329.1 pkt/s
11/04/2011	703.3 Kbits/s	156.4 pkt/s	25,8 Mbits/s	2628.4 pkt/s
12/04/2011	1,1 Mbits/s	194.5 pkt/s	25,8 Mbits/s	2310.7 pkt/s
15/04/2011	1,1 Mbits/s	242 pkt/s	22,7 Mbits/s	2847.6 pkt/s
16/04/2011	1,2 Mbits/s	240.6 pkt/s	24,7 Mbits/s	1052.3 pkt/s
17/04/2011	952,8 KMbits/s	226.1 pkt/s	8,7 Mbits/s	3578.9 pkt/s
18/04/2011	2,4 Mbits/s	505.1 pkt/s	26,9 Mbits/s	2487.8 pkt/s
19/04/2011	1,9 Mbits/s	529.7 pkt/s	22,1 Mbits/s	2487.8 pkt/s

Fuente: Reporte del software PTRG Network Monitor

En el Promedio de carga de la red y el pico en la carga de la red, de la tabla N°01, se puede apreciar que el día de mayor tráfico es el lunes 8 de abril del 2011 seguido de los días 9 y 19 del mismo mes.
La gráfica N°02 representa el resultado de la carga de la red esquematizado en barras para su mayor entendimiento.

Carga promedio de la red de Empresa Editora El Comercio – Planta Norte



Fuente: Reporte de PTRG.
Elaboración: Elaboración propia

En la gráfica N°02 se puede apreciar que existe una abrumada carga de red el día 08 de y el 19 de abril, esto genera los picos altos de tráfico en estos días, provocando perdida de señal y mayor lentitud de la red.

Este aumento de la tasa de datos enviados y recibidos de estos días se debe a que el día viernes 08 de abril, hubo mayor envío de información de los corresponsales y se aumento el número de páginas por Suplementos Comerciales.

Se complementa esta situación con algunas estadísticas de las interrupciones de la conexión tomadas también en el mes de abril del 2011 en las oficinas de la empresa.
Para la elaboración de esta tabla se ha tomado cuatro semanas del mes de abril, basada en el reporte semanal de quejas de la empresa, la referida tabla está ilustrada en la tabla N°02.

Tabla Nº 02 Cuadro de interrupciones de conexión en el mes de abril-2011

Semana	Días	Hora		
		7:00am -10:00am	10:00am-1:00pm	5:00pm- 9:00pm
1era semana	Lunes		X	X
	Martes			X
	Miércoles			X
	Jueves		X	X
	Viernes			X
	Sábado			X
	Domingo			X
2da semana	Lunes			
	Martes			X
	Miércoles			

	Jueves	X		X
	Viernes			X
	Sábado			X
	Domingo			
3ra semana	Lunes	X		X
	Martes	X		X
	Miércoles			
	Jueves			X
	Viernes			
	Sábado			X
	Domingo			X
4ta semana	Lunes		X	
	Martes			X
	Miércoles			
	Jueves			X
	Viernes			X
	Sábado			X
	Domingo			

Fuente: Reporte semanal de la empresa
Elaboración: elaboración propia

Donde se puede apreciar que ocurre por lo menos una interrupción por semana, que ocasiona malestar en los trabajadores de esta oficina, cuando esto ocurre los trabajadores amontonan los pedidos hasta que el servicio retorne, perdiendo tiempo en pasar al sistema después.

Al ocurrir los defectos mencionados anteriormente, ocasionan muchos inconvenientes tales como: el no funcionamiento de los aplicativos de la organización conectados al servidor, que ocasionan malestar y pérdida de tiempo en los usuarios, que tienen que esperar hasta que se restablezca la conexión, este problema causa pérdida de tiempo y hasta de dinero.

Ante esto surge la necesidad de evaluar y aplicar metodologías de diseño de red, que harán que estudiemos las condiciones de la organización, y de acuerdo a ello, proponer una adecuada arquitectura de la red con los dispositivos, medios y topologías que ayuden para un buen diseño de la red. Puesto que este dará soporte a muchos servicios vitales para la organización.

Este estudio también nos dirá las necesidades para implementar una red con todos los servicios que esta desea (infraestructura de voz, voz-IP, telefonía-IP, etc.), de acuerdo a las necesidades que se presenten y tomando en cuenta principalmente con los recursos con el que se dispone.

ANEXO III

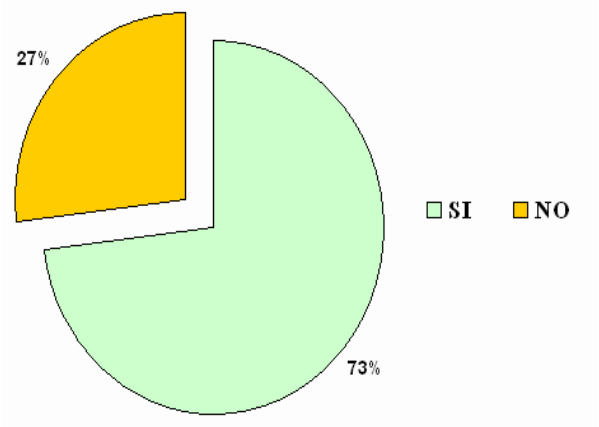
Medición de percepción de la seguridad de la red en el diario El Comercio Planta Norte.

Esta medición se hizo en base a encuestas para determinar los recursos que dispone el usuario para poder evitar el acceso no autorizado a su computador y la información que en él se encuentra.

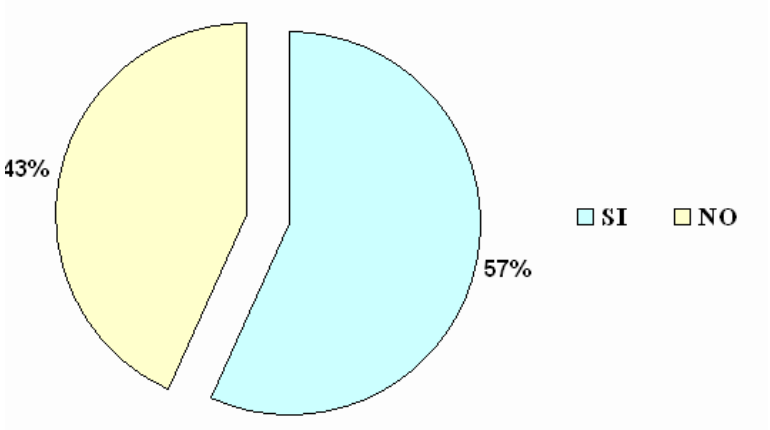
Para desarrollar esta medición encuesta, se le aplica a muestra de 18 usuarios de la Empresa Editora El Comercio – Planta Norte y Oficinas Descentralizadas de Piura, Chiclayo y Trujillo, para determinar el nivel de ocurrencia de problemas relacionados a la Seguridad.

Encuesta.

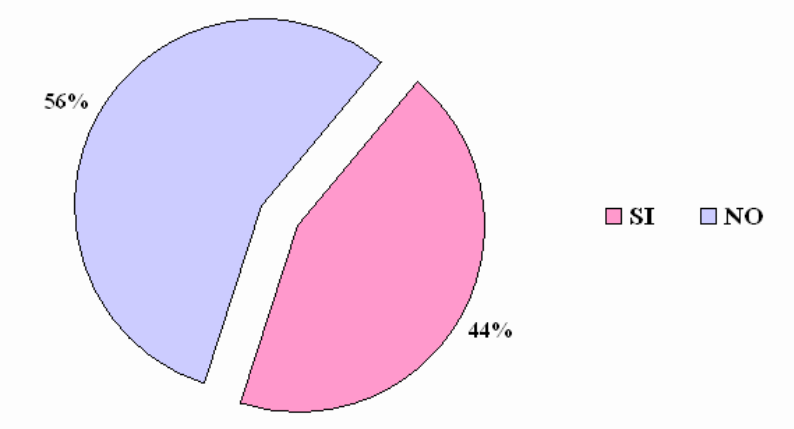
1.- ¿Alguna vez ha podido, de manera no intencional revisar archivos de usuarios de otras PCs?



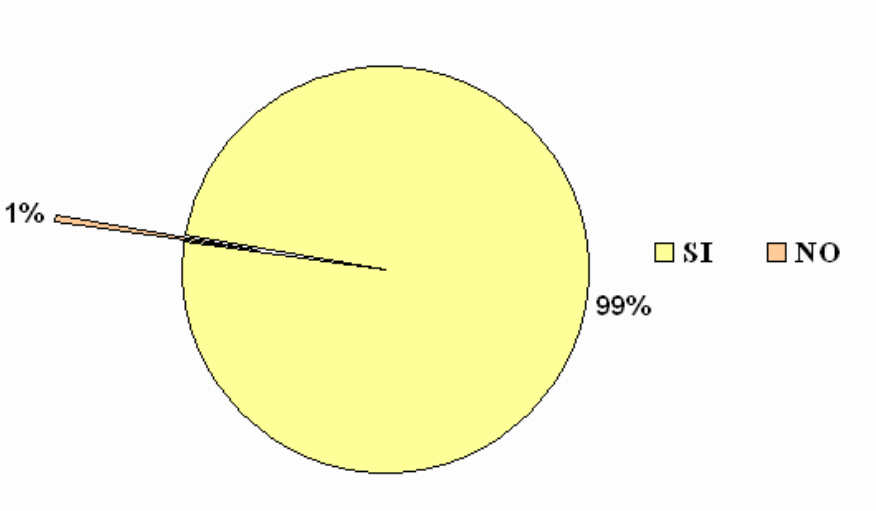
2.- ¿Alguna vez han entrado en tu computador personal y han robado alguna información?



3.- ¿Alguna vez se ha filtrado tu información periodística a otros medios?



4.- ¿Alguna vez se te ha perdido algún archivo cuando lo has compartido a través de la red?



ANEXO IV

Cuadro Causa Efecto – Problemática Planta Norte

Ítem	Problema	Causa	Efecto
1	Retraso en el Proceso de Elaboración, y Edición de las notas de los diarios	Dificultad en la recepción de la información por parte de los corresponsales de las sucursales	Cierre de la Edición luego de la hora establecida
2	Retraso en la Diagramación y Diseño de los diarios	Lentitud de la ejecución del software Arkitex que se despliega bajo una arquitectura cliente/Servidor	Aumento del tiempo programado para las actividades de Diagramación y Diseño
3	No se puede imprimir en plotter a través de la red	Latencia de la red en determinadas horas	Se pierde la conexión en forma intermitente y en ocasiones permanente
4	No se puede subir al servidor archivos gráficos, videos	Saturación del tráfico de la Red LAN	Manipulación de archivos a través de medios externos: USB, HD, etc. exponiendo a propagación de virus
5	El problema de un equipo activo de red afecta a los demás componentes	Red plana con Único dominio de broadcast	Extensión del dominio de broadcast a través de los equipos de la Red
6	Dificultad para enviar y descargar adjuntos en mensajes de correo	Aumento del tráfico de la información en horas pico (5:00 pm – 9:00 pm)	Degradación de la tasa de transferencia en las horas pico.
7	Demora y Complejidad para la determinación de problemas de red	Estructura de Red no documentada	Desorden en el crecimiento de la red además en la asignación de direcciones IP
8	Los usuarios pueden ver los recursos compartidos en toda la red de datos	Red sin segmentos lógicos en función a las áreas organizacionales	Información confidencial no protegida, dándose el riesgo de que otros usuarios puedan acceder a información sin estar autorizados.
9	Dificultad en comunicación por telefonía IP	Saturación del ancho de banda	Se presenta retardo en la transmisión de voz en horas punta
10	Envío y recepción de datos entre la Planta Norte y las Oficinas descentralizadas de Piura, Chiclayo y Trujillo es no segura	Uso de correo electrónico comercial	Pérdida de información, intercepción de mensajes, sabotaje.

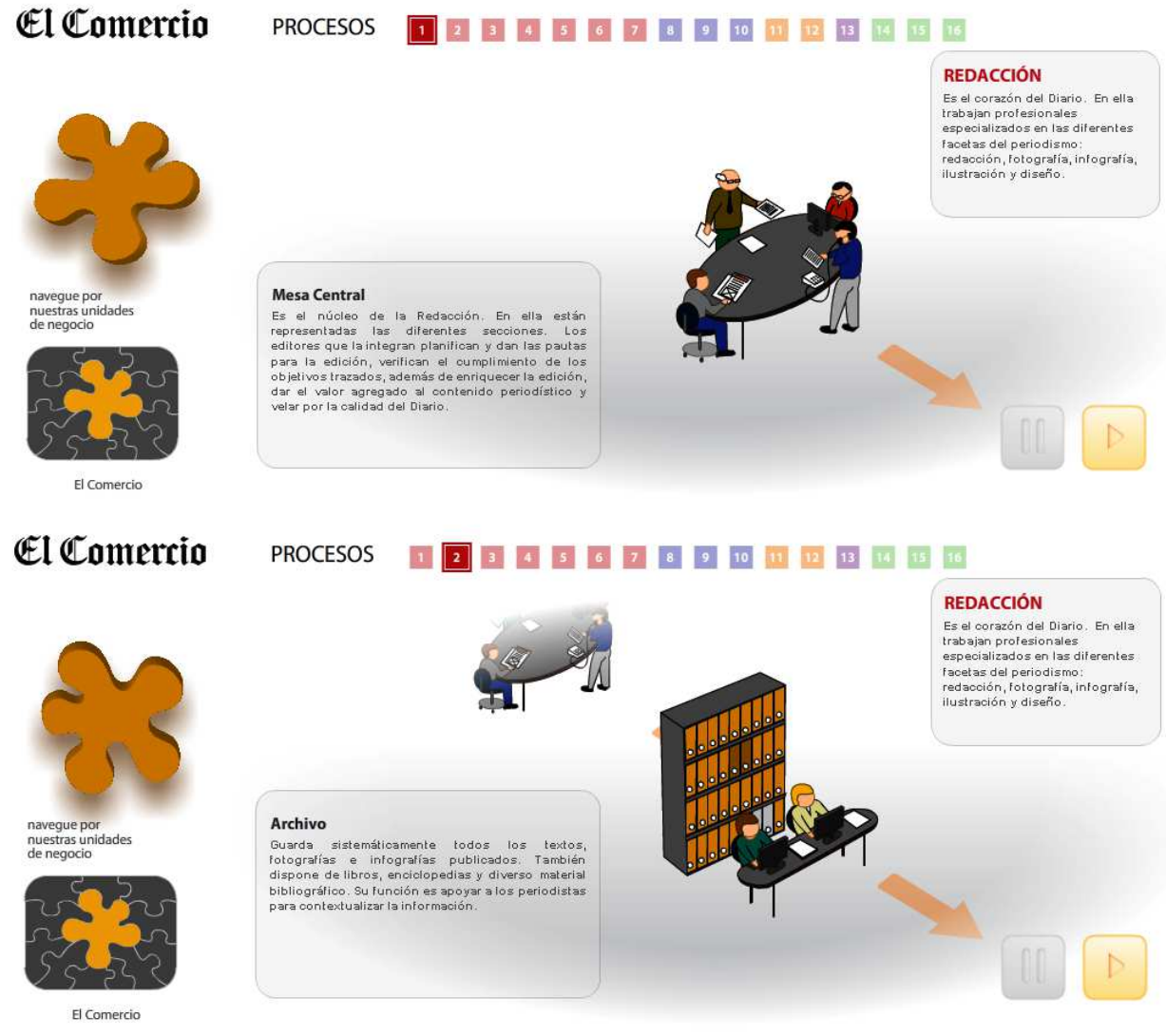
Cuadro Nº 23: Causa Efecto – Problemática Planta Norte

ANEXO V

SECUENCIA DEL PROCESO PERIODISTICO DE LOS PRODUCTOS DE LA PLANTA NORTE DEL GRUPO EL COMERCIO

Figura Nº 57: Secuencia Infografía 2011

Se resumen en 16 procesos o etapas, los pasos a seguir para la elaboración de cualquier producto dentro de la Familia del Grupo de El Comercio.



El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por
nuestras unidades
de negocio

El Comercio

REDACCIÓN

Es el corazón del Diario. En ella trabajan profesionales especializados en las diferentes facetas del periodismo: redacción, fotografía, infografía, ilustración y diseño.

Redacción

Recaba información desde diferentes fuentes, la analiza y trabaja de acuerdo con un plan de comisiones confeccionado por los editores de cada sección. La Redacción está dividida en secciones: Política, Lima, Perú, Mundo, Contracorriente, Deporte Total, Economía, Vida y Futuro y Luces. Se edita también los suplementos El Dominical, ¡Vamos!, Casa y Más, Mi Hogar, Día 1, Mi Negocio, Empleos y la revista Somos.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por
nuestras unidades
de negocio

El Comercio

REDACCIÓN

Es el corazón del Diario. En ella trabajan profesionales especializados en las diferentes facetas del periodismo: redacción, fotografía, infografía, ilustración y diseño.

Sistemas

Presta apoyo tecnológico al área de Redacción. Hace seguimiento de los equipos informáticos para garantizar su operatividad.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por
nuestras unidades
de negocio

El Comercio

REDACCIÓN

Es el corazón del Diario. En ella trabajan profesionales especializados en las diferentes facetas del periodismo: redacción, fotografía, infografía, ilustración y diseño.

Área gráfica

Es la parte de la Redacción encargada del periodismo visual. Sus integrantes son los responsables de crear las imágenes que acompañan la noticia. Está integrada por tres secciones: Fotografía, infografía e ilustración y diseño

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

REDACCIÓN

Es el corazón del Diario. En ella trabajan profesionales especializados en las diferentes facetas del periodismo: redacción, fotografía, infografía, ilustración y diseño.

Edición on line

Elabora la edición electrónica del Diario. Los usuarios de Internet acceden a los principales hechos ocurridos en el país y en el mundo, con actualizaciones constantes a lo largo del día.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

REDACCIÓN

Es el corazón del Diario. En ella trabajan profesionales especializados en las diferentes facetas del periodismo: redacción, fotografía, infografía, ilustración y diseño.

Comunicaciones

Hace rastreo permanente de los medios de comunicación radiales y televisivos y alerta sobre los últimos acontecimientos. También organiza las unidades móviles que trasladan a los periodistas.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

PUBLICIDAD

Es la parte de la empresa encargada de dar servicio a los anunciadores. Los avisos publicitarios son de dos tipos: los preferenciales, que pueden ir de acuerdo al cliente y normas del Diario; y los clasificados.

Recepción de avisos

Los clientes pueden poner un aviso en el Diario ya sea personalmente, en las sedes comerciales de Lima y San Isidro en las 80 agencias concesionarias o a través de teléfono.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

PUBLICIDAD

Es la parte de la empresa encargada de dar servicio a los anunciadores. Los avisos publicitarios son de dos tipos: los preferenciales, que pueden de acuerdo al cliente y normas Diario; y los clasificados.

Avisos

Procesan los avisos que proponen los clientes para que cumplan las características técnicas de impresión.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

PUBLICIDAD

Es la parte de la empresa encargada de dar servicio a los anunciadores. Los avisos publicitarios son de dos tipos: los preferenciales, que pueden ir de acuerdo al cliente y normas del Diario; y los clasificados.

Diseño Publicitario

Es el área de creativos publicitarios. Este equipo hace el arte de los avisos, también recibe aquellos avisos enviados por las agencias para que sean adaptados al formato del Diario.

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

El Comercio

PRE-PRENSA

Se encarga de la parte productiva del proceso de elaboración del periódico. En esta área convierten las páginas digitales en planchas de aluminio que son colocadas en la rotativa donde es impreso el Diario.

Sistema AGFA

Es un sistema que procesa de manera automática las páginas de la Redacción y de Publicidad para luego hacer la imposición.

El Comercio

El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por
nuestras unidades
de negocio

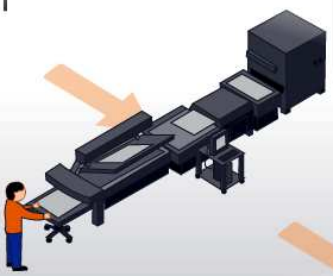
El Comercio

PRE-PRENSA

Se encarga de la parte productiva del proceso de elaboración del periódico. En esta área convierten las páginas digitales en planchas de aluminio que son colocadas en la rotativa donde es impreso el Diario.

CTP (Computer to Plate).

Es el proceso para producir la página en un soporte que permita incorporarla a la rotativa.



El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por
nuestras unidades
de negocio

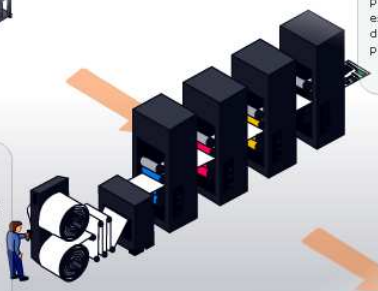
El Comercio

ROTATIVA

Esta área está encargada de realizar la impresión de los productos manteniendo estándares de colores y la calidad de impresión necesaria para los periódicos.

Rotativa

La rotativa se compone de ocho unidades o torres. Para conseguir todo el espectro cromático y así imprimir las páginas en color es necesario combinar cuatro tipos de tinta. El proceso para las páginas en blanco y negro se simplifica a una.



El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

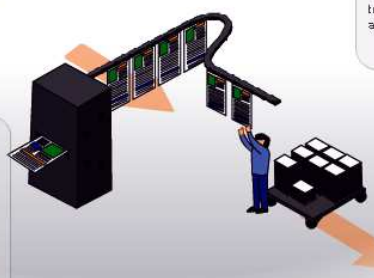
El Comercio

CIRCULACIÓN

Culminado el proceso de producción del Diario, esta área recibe los ejemplares impresos y los distribuye por todo el país. El transporte se hace por tierra o aire, de acuerdo con la demanda.

Despacho

Es el último paso del proceso de impresión del periódico. Los ejemplares son transportados a través de pinzas individuales desde la rotativa, y se entrega en la cantidad exacta a cada aplicador, según su destino final.



El Comercio

PROCESOS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

navegue por nuestras unidades de negocio

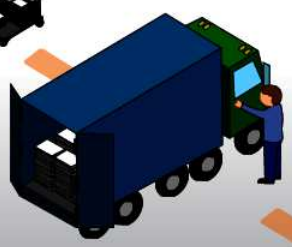
El Comercio

CIRCULACIÓN

Culminado el proceso de producción del Diario, esta área recibe los ejemplares impresos y los distribuye por todo el país. El transporte se hace por tierra o aire, de acuerdo con la demanda.

Circulación

Se encargan de repartir los ejemplares por todo el territorio nacional. En total existen en el país 274 puntos de distribución.



ANEXO VI

CONIGURACIÓN ROUTER RCOMERCIO

```
Building configuration...

Current configuration : 6831 bytes

version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname RCOMERCIO

enable secret 5 $1$mERr$g9AtCrDRbrZ7HXvSfWwI0/

ip dhcp pool adm-comer
 network 172.16.1.64 255.255.255.240
 default-router 172.16.1.65
 option 150 ip 172.16.1.65
ip dhcp pool VOZ
 network 172.16.1.0 255.255.255.224
 default-router 172.16.1.1
 option 150 ip 172.16.1.1
ip dhcp pool seguridad
 network 172.16.1.176 255.255.255.248
 default-router 172.16.1.177
 option 150 ip 172.16.1.177
ip dhcp pool preprensa
 network 172.16.1.128 255.255.255.248
 default-router 172.16.1.129
 option 150 ip 172.16.1.129
ip dhcp pool redaccion
 network 172.16.1.32 255.255.255.224
 default-router 172.16.1.33
 option 150 ip 172.16.1.33
ip dhcp pool almacen
 network 172.16.1.160 255.255.255.248
 default-router 172.16.1.161
 option 150 ip 172.16.1.161
ip dhcp pool publicidad
 network 172.16.1.168 255.255.255.248
 default-router 172.16.1.169
 option 150 ip 172.16.1.169
ip dhcp pool rotativa
 network 172.16.1.136 255.255.255.248
 default-router 172.16.1.137
 option 150 ip 172.16.1.137
```

Configuración de los POOLS DHCP para cada subred

```
ip dhcp pool despacho
network 172.16.1.144 255.255.255.248
default-router 172.16.1.145
option 150 ip 172.16.1.145
ip dhcp pool mantenimiento
network 172.16.1.152 255.255.255.248
default-router 172.16.1.153
option 150 ip 172.16.1.153
ip dhcp pool circulacion
network 172.16.1.80 255.255.255.240
default-router 172.16.1.81
option 150 ip 172.16.1.81
ip dhcp pool invitado
network 172.16.1.112 255.255.255.240
default-router 172.16.1.113
option 150 ip 172.16.1.113
```

```
aaa new-model

aaa authentication login default group radius none
aaa authentication login telnet_lines group radius
```

Creamos un nuevo modelo AAA para autenticar usuarios de acceso remoto mediante RADIUS

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.1.177 255.255.255.248
 ip access-group 100 in

interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.1.129 255.255.255.248
 ip access-group 102 in

interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.1.65 255.255.255.240
 ip access-group 101 in

interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.1.33 255.255.255.224
 ip access-group 103 in

interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.16.1.169 255.255.255.248
 ip access-group 106 in
```

Creación de subinterfaces con su dirección ip.
Algunas interfaces permiten el ingreso de ACL

```
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 172.16.1.137 255.255.255.248
 ip access-group 107 in

interface FastEthernet0/0.70
 encapsulation dot1Q 70
 ip address 172.16.1.145 255.255.255.248
 ip access-group 108 in

interface FastEthernet0/0.80
 encapsulation dot1Q 80
 ip address 172.16.1.81 255.255.255.240
 ip access-group 110 in

interface FastEthernet0/0.90
 encapsulation dot1Q 90
 ip address 172.16.1.153 255.255.255.248
 ip access-group 109 in

interface FastEthernet0/0.99
 encapsulation dot1Q 99 native
 ip address 172.16.99.1 255.255.255.248

interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.16.1.161 255.255.255.248
 ip access-group 105 in

interface FastEthernet0/0.110
 encapsulation dot1Q 110
 ip address 172.16.1.97 255.255.255.240

interface FastEthernet0/0.120
 encapsulation dot1Q 120
 ip address 172.16.1.1 255.255.255.224

interface FastEthernet0/0.130
 encapsulation dot1Q 130
 ip address 172.16.1.113 255.255.255.240
 ip access-group 104 in

access-list 100 deny tcp 172.16.1.176 0.0.0.7 any eq telnet
access-list 100 permit ip any any
access-list 101 deny tcp 172.16.1.64 0.0.0.15 any eq telnet
access-list 101 permit ip any any
access-list 102 deny tcp 172.16.1.128 0.0.0.7 any eq telnet
access-list 102 permit ip any any
access-list 103 deny tcp 172.16.1.32 0.0.0.31 any eq telnet
```

Creación de ACL para las áreas que no pueden administrar el router

```
access-list 103 permit ip any any
access-list 104 deny tcp 172.16.1.112 0.0.0.15 any eq telnet
access-list 104 permit ip any any
access-list 105 deny tcp 172.16.1.160 0.0.0.7 any eq telnet
access-list 105 permit ip any any
access-list 106 deny tcp 172.16.1.168 0.0.0.7 any eq telnet
access-list 106 permit ip any any
access-list 107 deny tcp 172.16.1.136 0.0.0.7 any eq telnet
access-list 107 permit ip any any
access-list 108 deny tcp 172.16.1.144 0.0.0.7 any eq telnet
access-list 108 permit ip any any
access-list 109 deny tcp 172.16.1.152 0.0.0.7 any eq telnet
access-list 109 permit ip any any
access-list 110 deny tcp 172.16.1.80 0.0.0.15 any eq telnet
access-list 110 permit ip any any

radius-server host 172.16.1.99 auth-port 1645 key comercio

telephony-service
max-ephones 20
max-dn 20
ip source-address 172.16.1.1 port 2000
auto assign 1 to 20

ephone-dn 1
number 7340

ephone-dn 2
number 7341

ephone-dn 3
number 7342

ephone-dn 4
number 7343

ephone-dn 5
number 7344

ephone-dn 6
number 7345

ephone-dn 7
number 7346

ephone-dn 8
number 7347

ephone-dn 9
```

Identificamos al servidor de autenticación RADIUS, el número de puerto y la clave del radius

- Configuración del Servicio de Telefonía en el Router Rcomercio, cumpliendo la función de CME (CALL MANAGER EXPRESS).
- Identificamos la cantidad de teléfonos y sus respectivos números (dn)
- Luego configuramos por teléfono su respectivo numero.

```
number 7348

ephone-dn 10
 number 7349

ephone-dn 11
 number 7350

ephone-dn 12
 number 7351

ephone-dn 13
 number 7352

ephone-dn 14
 number 7353

ephone-dn 15
 number 7354

ephone-dn 16
 number 7360


ephone 1
 device-security-mode none
 mac-address 0002.4A7C.AB97
 type 7960
 button 1:10

ephone 2
 device-security-mode none
 mac-address 00E0.B05B.2A48
 type 7960
 button 1:8

ephone 3
 device-security-mode none
 mac-address 0050.0FB7.7711
 type 7960
 button 1:9

ephone 4
 device-security-mode none
 mac-address 0090.0CB0.593D
 type 7960
 button 1:15

ephone 5
```

Registro automático de los teléfonos ip con su respectiva dirección MAC

```
 device-security-mode none
 mac-address 0001.42B5.5976
 type 7960
 button 1:11

ephone 6
 device-security-mode none
 mac-address 0060.5C8E.E3BC
 type 7960
 button 1:4

ephone 7
 device-security-mode none
 mac-address 0060.2F2A.0725
 type 7960
 button 1:5

ephone 8
 device-security-mode none
 mac-address 0004.9A39.C574
 type 7960
 button 1:2

ephone 9
 device-security-mode none
 mac-address 0060.475D.1789
 type 7960
 button 1:3

ephone 10
 device-security-mode none
 mac-address 00E0.F921.5739
 type 7960
 button 1:1

ephone 11
 device-security-mode none
 mac-address 0060.7018.9A6B
 type 7960
 button 1:7

ephone 12
 device-security-mode none
 mac-address 000C.85E8.E0CD
 type 7960
 button 1:12

ephone 13
 device-security-mode none
```

```
 mac-address 0003.E472.6B4A
 type 7960
 button 1:14

ephone 14
 device-security-mode none
 mac-address 0000.0C91.75E7
 type 7960
 button 1:13

ephone 15
 device-security-mode none
 mac-address 0040.0BC0.1BE9
 type 7960
 button 1:6

ephone 16
 device-security-mode none
 mac-address 0060.5C66.52E4
 button 1:16

line con 0
line vty 0 4
 login authentication telnet_lines
```

Activamos las líneas virtuales e indicamos el acceso mediante el nombre telnet_lines que indicamos anteriormente en el RADIUS

CONFIGURACIÓN SWITCH CAPA 3 (CORE)

```
Building configuration...

Current configuration : 2077 bytes

version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW-CORE


enable secret 5 $1$mERr$g9AtCrDRbrZ7HXvSfWwI0/


interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/5
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/6
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/7
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/8
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/9
 switchport access vlan 110
 switchport mode access

interface FastEthernet0/10
 switchport access vlan 130
 switchport mode access

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18
```

```
interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23
 channel-protocol lacp
 channel-group 2 mode active
 switchport trunk native vlan 99

interface FastEthernet0/24
 channel-protocol lacp
 channel-group 5 mode active
 switchport trunk native vlan 99

interface GigabitEthernet0/1
 channel-protocol lacp
 channel-group 5 mode active
 switchport trunk native vlan 99

interface GigabitEthernet0/2
channel-protocol lacp
channel-group 2 mode active
switchport trunk native vlan 99

interface Port-channel 2

interface Port-channel 5

interface Vlan1
no ip address
shutdown

interface Vlan99
ip address 172.16.99.2 255.255.255.248

ip classless
ip route 172.16.0.0 255.255.0.0 172.16.99.1


line con 0
login
line vty 0 4
login
line vty 5 15
login
```

CONFIGURACIÓN DE VLANS

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22
10   SEGURIDAD-COM                     active
20   PRE-PRENSA                        active
30   ADMIN-COMER                       active
40   REDACCION                         active
50   PUBLICIDAD                        active
60   ROTATIVA                          active
70   DESPACHO                          active
80   CIRCULACION                       active
90   MANTENIMIENTO                     active
99   ADMIN-RED                         active
100  ALMACEN                           active
110  SISTEMAS                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9
120  VOZ                               active
130  INVITADO                          active    Fa0/10
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SW-CORE#
```

CONFIGURACIÓN DEL SERVIDOR VTP

```
VTP Version                     : 2
Configuration Revision          : 470
Maximum VLANs supported locally: 1005
Number of existing VLANs        : 19
VTP Operating Mode              : Server
VTP Domain Name                 : comercio
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x01 0xBB 0x2E 0x4B 0x7D 0xB3 0x67 0xFD
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 172.16.99.2 on interface Vl99 (lowest numbered VLAN interface
found)
```

CONFIGURACIÓN DE SWITCH CLIENTE

```
Building configuration...

Current configuration : 2851 bytes

version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW.ACC1
enable secret 5 $1$mERr$g9AtCrDRbrZ7HXvSfWwI0/

interface FastEthernet0/1

interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access

interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access

interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos
```

Configuración de puertos con QOS para identificar la vlan de VOZ como prioritaria y la vlan de acceso

```
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access

interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access

interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/16
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/17
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos
```

```
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 120
 mls qos trust cos

interface FastEthernet0/19
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/20
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/21
 switchport access vlan 40
 switchport mode access

interface FastEthernet0/22
interface FastEthernet0/23

interface FastEthernet0/24
 switchport trunk native vlan 99
 channel-protocol lacp
 channel-group 5 mode active
 switchport mode trunk

interface GigabitEthernet1/1
 switchport trunk native vlan 99
 channel-protocol lacp
 channel-group 5 mode active
 switchport mode trunk

interface GigabitEthernet1/2
interface Port-channel 5
 switchport mode trunk

interface Vlan1
 no ip address
 shutdown
interface Vlan99
 ip address 172.16.99.3 255.255.255.248
ip default-gateway 172.16.99.1

line con 0
line vty 0 4
 login
line vty 5 15
 login
```

Configuración de enlaces troncales y además GigaBitEthernetChannel (Agregados de Enlace) asegurando una rápida transmisión de datos con el protocolo LACP

CONFIGURACIÓN DEL CLIENTE VTP QUE RECIBE LAS VLANS DEL SWITCH CORE

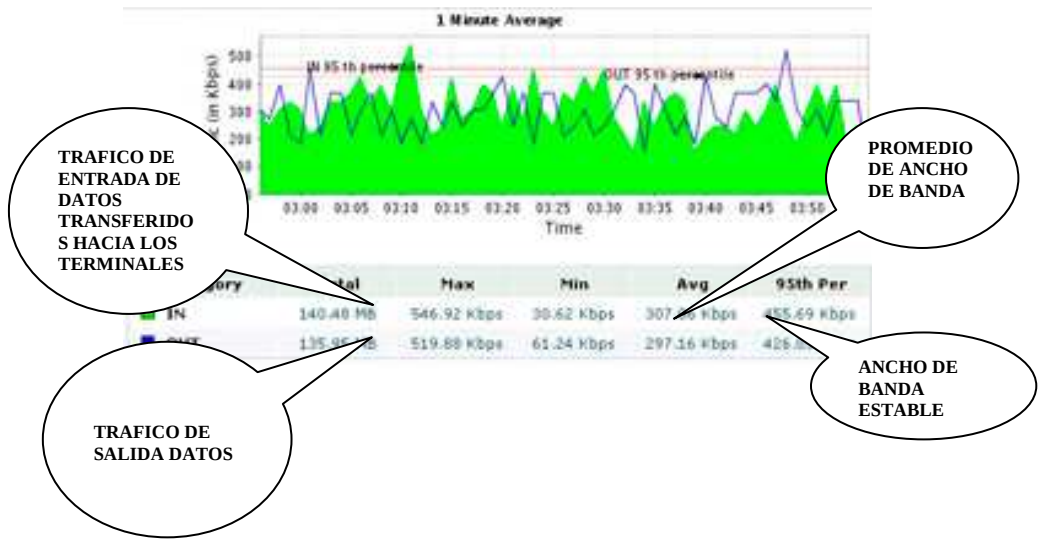
VTP Version : 2
Configuration Revision : 470
Maximum VLANs supported locally: 255
Number of existing VLANs : 19
VTP Operating Mode : Client
VTP Domain Name : comercio
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x01 0xBB 0x2E 0x4B 0x7D 0xB3 0x67 0xFD
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

ANEXO VII

Tráfico total de la Red Empresa Editora El Comercio – Planta Norte (PreTest)

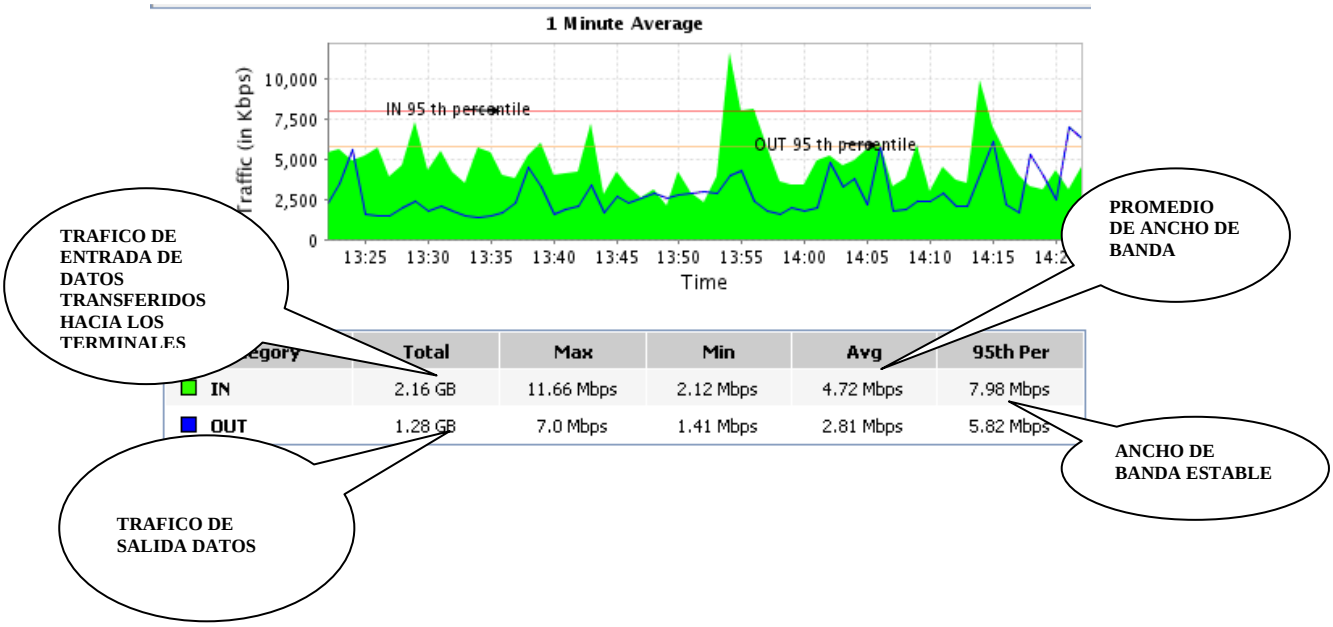
- En este primer cuadro observamos una medición de la Interfaz en el Servidor de mayor requerimiento y trabajo, el tráfico total de nuestra red, con un ancho de banda de 4.5 Mbps saturado por la fluctuación de información y sin estrategias Qos.

- Existe una cantidad de 140 MB de datos que fluyen a través de nuestra red donde no es posible que el Router Cisco 2800 Series identifique los diferentes tráficos y asigne prioridades, siendo dificultoso administrar una mayor tasa de información.



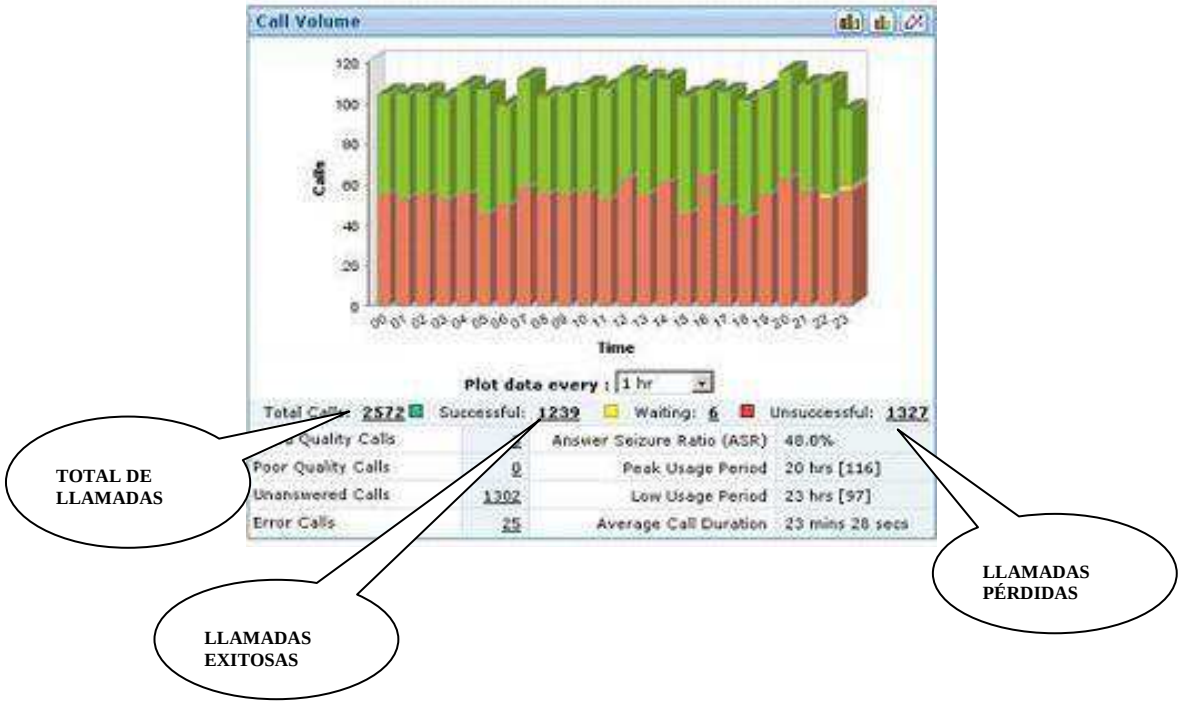
Tráfico total de la Red Empresa Editora El Comercio – Planta Norte (PostTest)

En este cuadro observamos que después de aplicar las estrategias de Rendimiento como QoS, LACP, etc., el ancho de banda mejoro en un 50% en horas pico, considerando que la plataforma o configuración actual permite a la Red, soportar mayores requerimientos de tráfico y recursos sin degradar la performance de la Red. Con ello hemos obtenido un Ancho de Banda estable.
Se aplicaron estrategias QoS, Lacp, Troncales Cisco, los cuales colaboran en la priorización y eficiencia del Tráfico de Data. La medición se realizó con el Software PTRG Network Monitor.



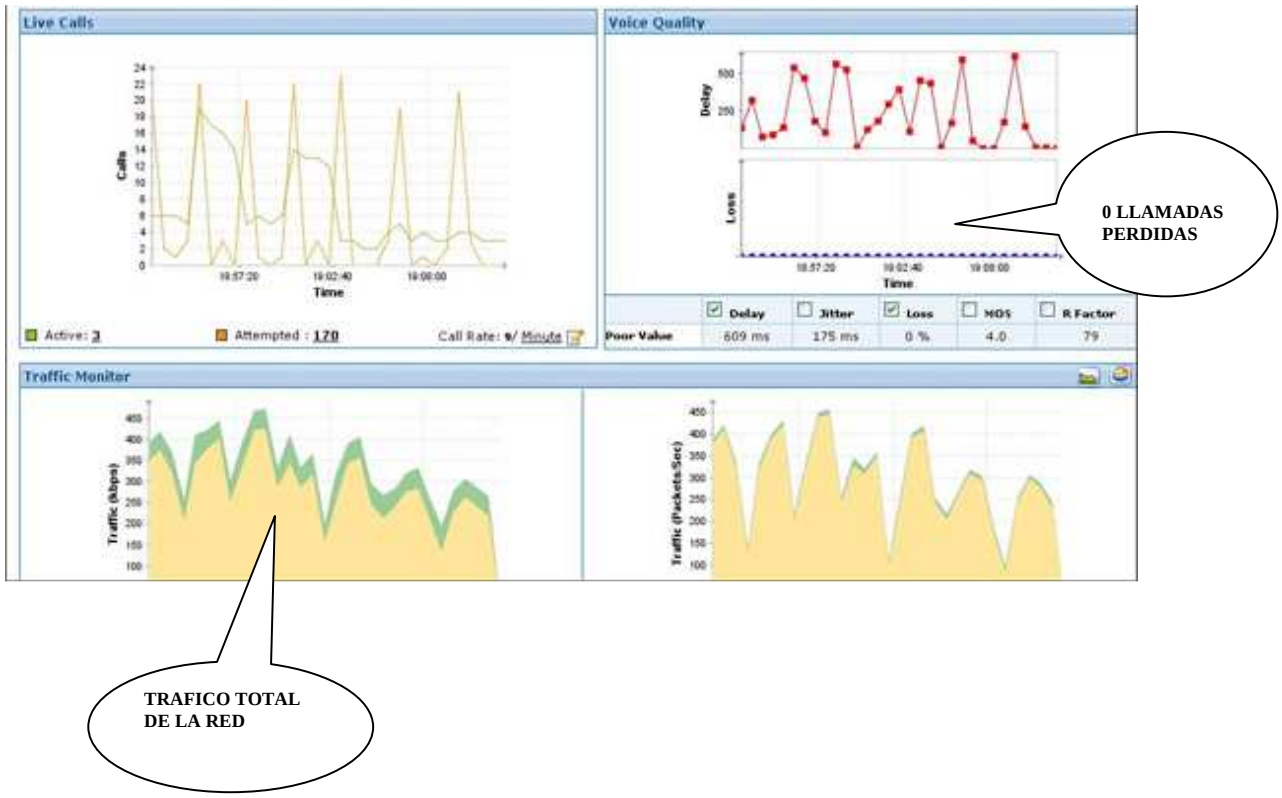
El aplicativo PTRG Network Monitor nos muestra que el Ancho de Banda estable es de 8 Mb/s, el cual denota capacidad para una mayor fluidez de información aún en horas críticas de los procesos (5:00pm – 10:00pm). La tasa de transferencia de entrada de Datos registra un promedio de 2.16 GB, mientras que la tasa de salida es de 1.28 GB, manteniéndose la Red dentro del rendimiento deseado.

Red Empresa Editora El Comercio Planta Norte - Tráfico de Voz sin QoS - PreTest



Los registros en el tráfico de voz, denotaban una problemática en la comunicación debido a la ausencia de Estrategias de QoS, provocando "perdida, cortes o fluctuación en las llamadas con Teléfonos IP, el cual representaba un promedio del 50 % según la gráfica.

Red Empresa Editora El Comercio Planta Norte - Tráfico de Voz sin QoS – PosTest



Después de la implementación de Estrategias QoS, el parámetro de interrupciones en la señal de Voz mostro un resultado satisfactorio, donde solo existe un retardo de 609 ms (microsegundos) que es un tiempo considerable en la mayoría de redes VoIp. Con esto podemos validar la hipótesis de que el uso de nuevas tecnologías y configuraciones basadas en estrategias de Rendimiento y Seguridad brindan beneficios operativos y son el soporte para las Estrategias Corporativas, disminuyendo las falencias de la Red y maximizando el uso racional de los recursos informáticos.

ANEXO VIII

PLAN DE CONTINGENCIA EMPRESA EDITORA EL COMERCIO PLANTA NORTE

INTRODUCCIÓN

El presente Plan de Contingencia es implementado como parte de una solución para la PROPUESTA DE SEGMENTACIÓN CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO – PLANTA NORTE, para mantener la continuidad de transmisión de datos entre las sedes Principales (Lima: Planta Pando, San Isidro y Arequipa), generando enlaces alternativos, permitiendo así que la red sea tolerante a fallas.

La Red al poseer planes de respuesta ante la caída de las comunicaciones con la ciudad de Lima y Arequipa permite elevar la calidad de la misma, manteniendo siempre operativos los sistemas y automatizando los procesos, generando así que los trabajos informáticos se cumplan al 100 %, no repercutiendo en los ingresos económicos por posibles estancamientos de la Productividad

OBJETIVOS

Los objetivos del Plan de Contingencia PROPUESTA DE SEGMENTACIÓN CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO – PLANTA NORTE están basados en el cumplimiento de lo siguiente:

- Evaluar, analizar y prevenir los riesgos en nuestra red.
- Evitar la pérdida de conexión y por ende la perdida de datos.
- Generar enlaces alternativos.
- Evitar la pérdida de negocios a causa de fallas de red
- Entre otros

DESCRIPCIÓN DE LAS OPERACIONES

a) **Actividad y operación principal**

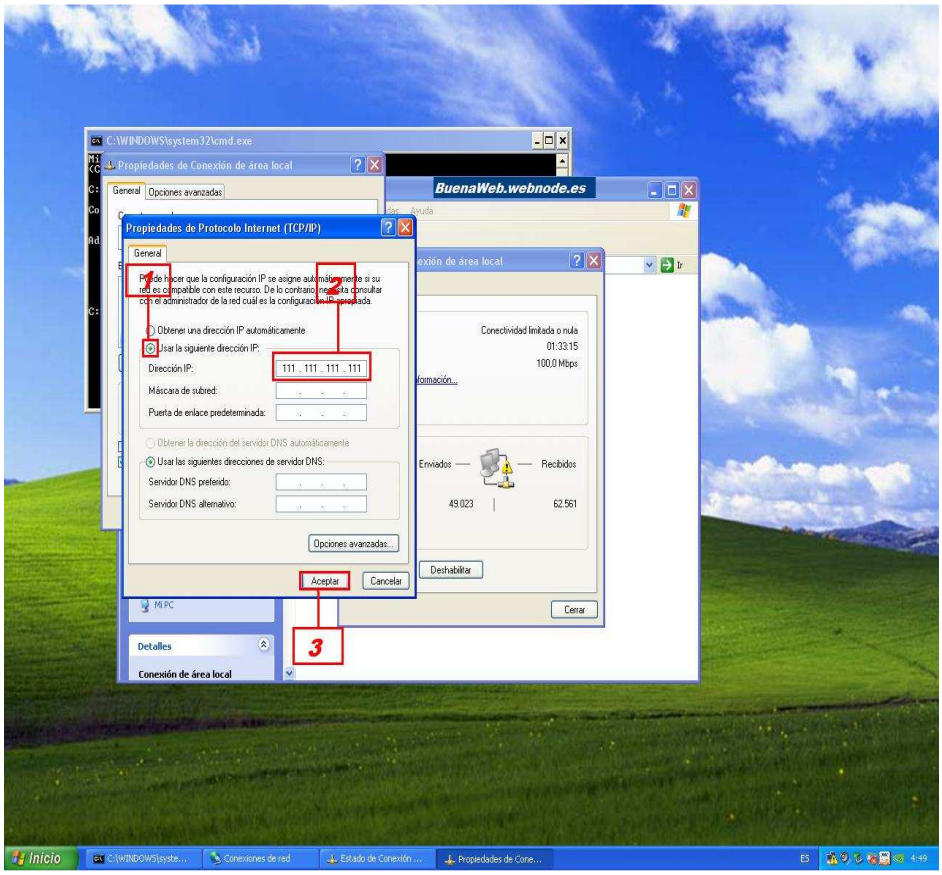
- La principal actividad del Plan de Contingencia es la creación de enlaces alternativos.

La operación comienza con el establecimiento de un enlace alternativo a través de un modem dedicado provisto por un ISP (Movistar)

- Otra actividad es manejar un enlace wireless a través de 2 modem's USB (Movistar y Claro), que entra en funcionamiento cuando posiblemente haya una falla en la red externa.
- Asimismo se cuenta con un conmutador Cisco alternativo modelo 3560 – 48 puertos y un Switch D-Link de 24 puertos. Por lo que se cuenta con Backups de cada configuración de los equipos intermedios de la red, donde estos se cargan a un nuevo dispositivo según lo amerite el caso, **esto respondiendo a fallas internas en la Red.**

b) Diagrama de Operación.

Se selecciona equipos del área de Sistemas y se cambia los valores IP de la maquina, donde le damos valores predeterminados del enlace Speedy:



- De esta manera el numero de IP asignado sería el siguiente:

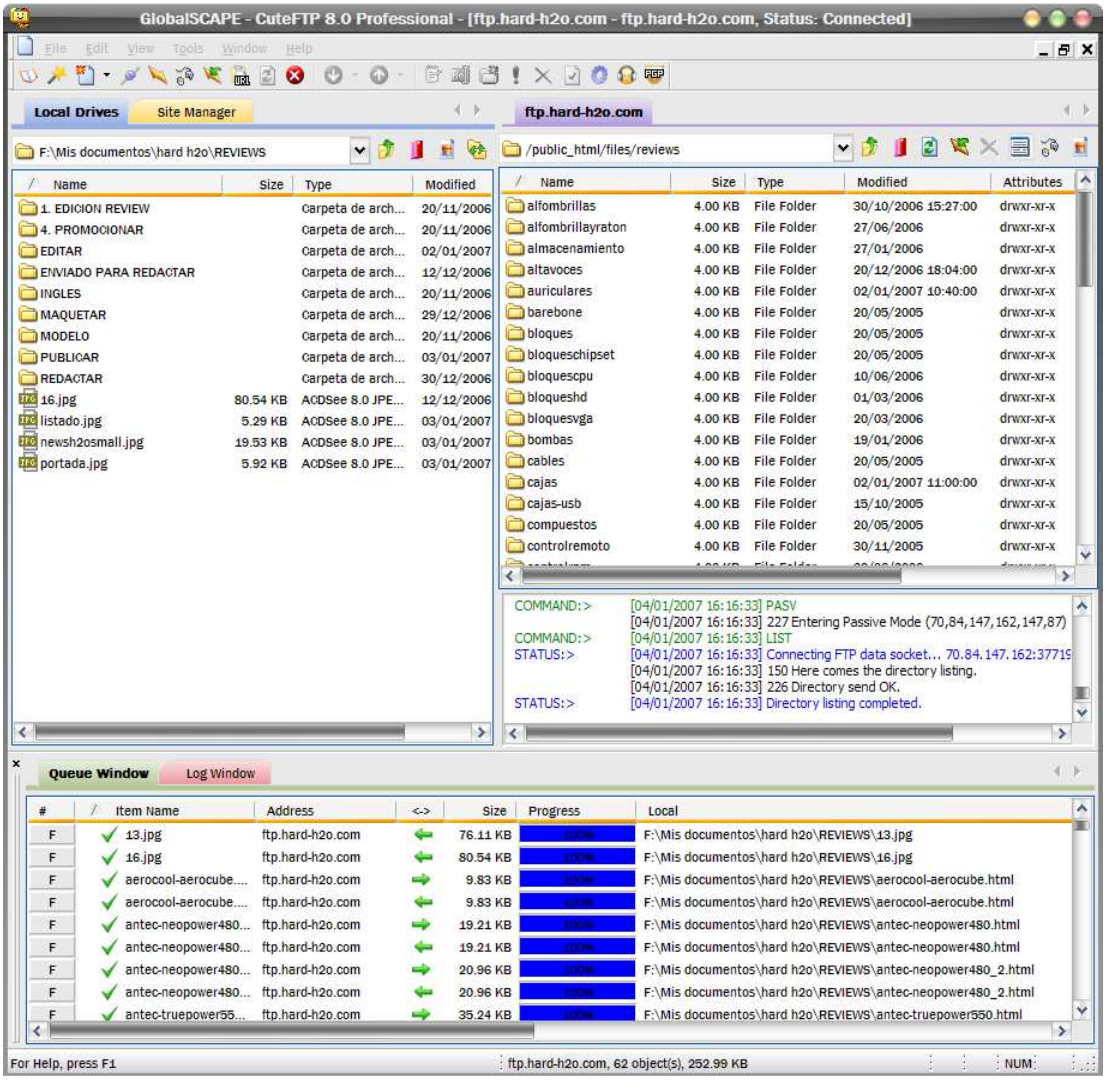
IP: 192.168.1. (x,…)

Mascara Subred: 255.255.255.0

Puerta Enlace: 192.168.1.1

DNS: 200.48.225.130
200.48.225.146

0 Donde inicializamos el aplicativo Cute FTP en la maquina local y al mismo tiempo en las Pc's de otras sedes:



- De esta manera tanto los enlaces alambricos (conexión speedy) e inalámbricos(Modem USB Movistar y Claro), trabajan conjuntamente para soportar el flujo e intercambio de información para los Diarios.

Conclusión:

El enlace de Línea Dedicada con el que actualmente se conecta la Planta Chiclayo hacia las demás sedes principales ubicadas en la ciudad de Lima y Arequipa, están propensos a presentar averías en su estructura física y lógica, el cual se da aproximadamente 3 veces al año.

Estos percances en la comunicación externa son respondidos por los aplicativos y equipos de comunicación: Aplicativo FTP, Modem's Movistar y Claro, Línea Speedy – Router.

De la misma manera contar con conmutadores responden a la necesidad resolver problemas de conectividad internos, apoyados en backups de las configuraciones de los equipos, ahorrando tiempo en volver a configurar cada nuevo equipo conectado a la Red.