UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TESIS DE GRADO

TEMA:

ADMINISTRACIÓN DE REDES LAN Y WAN UTILIZANDO CISCO WORKS SOBRE TECNOLOGÍAS DE ALTA VELOCIDAD

APLICATIVO:

DISEÑO, CONFIGURACIÓN E IMPLEMENTACIÓN DE LA HERRAMIENTA DE MONITOREO DE RED CISCO WORKS Y REGLAMENTACIÓN DEL USO DE SERVICIOS EN PETROINDUSTRIAL FILIAL DE PETROECUADOR

AUTOR:

MARCO ANTONIO GALIANO YÉPEZ

DIRECTOR:

ING. JORGE CARAGUAY

IBARRA, NOVIEMBRE 2007

CERTIFICACIÓN

Certifico que el presente trabajo, previo a la obtención del Título de Ingeniero en Sistemas Computacionales, fue desarrollado por Marco Antonio Galiano Yépez, bajo mí supervisión.

_____

Ing. Jorge Caraguay

DIRECTOR DE TESIS

DEDICATORIA

A Dios y la Virgen por darme la vida y guiarme por el camino correcto, darme la fuerza para seguir luchando y alcanzar mis metas e ideales.

A mis padres Arnulfo y Oliva por ser quienes con su cariño, amor y dedicación me enseñaron los valores de honestidad, trabajo y humildad, con sus consejos y total apoyo supieron darme el ejemplo de constancia y superación.

A Mi Esposa Rocío por brindarme todo su Amor, Cariño y Comprensión y estar siempre pendiente de mí.

A Mi Adorada Hija Melany Dannaé por ser la luz de mis ojos y reflejar todo mi amor y orgullo en su sonrisa.

Marco Antonio Galiano.

AGRADECIMIENTO

A Dios, a Mis Padres por brindarme la oportunidad de poder estudiar y obtener un título profesional para enfrentar el futuro con mejores expectativas y oportunidades.

A Mi Esposa Rocío por su paciencia y comprensión durante el tiempo que tomó desarrollar este proyecto de titulación.

Al Ing. Jorge Caraguay por su guía y tutoría en el desarrollo de este proyecto de titulación.

A Mi Tía Rubí y Mi Prima Xiomara por haberme abierto las puertas de su hogar y el apoyo incondicional que me han brindado.

Al Ing. Napoleón Córdova por su apertura y colaboración durante el desarrollo de este proyecto y su confianza en el trabajo.

Marco Antonio Galiano.

RESUMEN

La administración de las redes de comunicación, sean estas LAN, MAN ó WAN hoy en día es de primordial importancia para todas las instituciones o empresas que dependen del flujo y disponibilidad de su activo más importante, la información.

Considerando el gran valor alcanzado por los sistemas de comunicación y su paulatino crecimiento, hace indispensable que sobre ellos se instale y reglamente un adecuado sistema de administración con el objetivo de optimizar el uso de los recursos que pone a disposición de sus usuarios una empresa enfocándose en la meta de obtener el mayor rédito y productividad posibles.

Con estos antecedentes el presente proyecto de grado hace un estudio de las principales tecnologías de alta velocidad para redes y sistemas de comunicación, además realiza un análisis de la herramienta de administración y monitoreo de equipos activos y recursos de red CISCO WORKS que dispone Petroindustrial, Filial de Petroecuador.

El primer y segundo capítulo comprende un estudio de las principales tecnologías de alta velocidad para las redes de comunicación, tendencias, características principales, ventajas y desventajas y su evolución a lo largo de la historia.

El tercer capítulo presenta información de la estructura organizacional de Petroindustrial, el enfoque de la Unidad de Sistemas dentro de esta filial de PETROECUADOR, y su lugar como empresa de industrialización de derivados.

El cuarto capítulo realiza un estudio de las tecnologías utilizadas dentro de Petroindustrial a nivel nacional dentro de sus sistemas de comunicación y de los proyectos tecnológicos que esta filial pretende implementar para mejorar su desempeño operacional.

El quinto capítulo resume la estructura de red LAN y WAN de Petroindustrial a nivel nacional, así como los problemas detectados dentro de los sistemas de comunicación, cuellos de botella y configuraciones actualmente aplicadas sobre sus equipos activos.

El sexto capítulo comprende un análisis técnico de los equipos de red, sus configuraciones operacionales y las tecnologías que estos soportan, enfocados en satisfacer las necesidades de los proyectos nuevos que la Filial pretende implementar.

El séptimo capítulo presenta información característica de la herramienta de Administración y Monitoreo de Red CISCO WORKS, sus características técnicas y de funcionamiento, sus módulos de trabajo y las configuraciones necesarias para monitorear y administrar redes LAN y WAN basadas en equipos de marca CISCO.

El octavo capítulo de este proyecto involucra la implementación y configuración de la herramienta CISCO WORKS sobre la red de datos de Petroindustrial. Además del diseño de un reglamento modelo para administración de servicios, recursos y equipos de red, así como su aplicación a través de esta herramienta con el fin de ofrecer una visión clara de cómo mejorar el rendimiento y performance de un sistema de comunicaciones como el instalado en esta empresa.

Finalmente en el noveno capítulo se presenta la verificación de la hipótesis, conclusiones y recomendaciones que han sido recopiladas durante todo el proceso de elaboración del presente proyecto, además algunos posibles temas para nuevos proyecto de tesis.

INTRODUCCIÓN

Una red, vista desde su nivel más básico, es la interconexión de dos equipos entre sí, mediante un medio físico; de tal manera que permitan compartir información entre ellos. Hoy en día, todas las redes sin importar lo sofisticadas que sean parten de este sencillo sistema; y aunque su interconexión no parezca extraordinaria, visto en el tiempo, este ha sido el mayor e importante logro del mundo de las comunicaciones.

Uno de los objetivos de las redes es compartir recursos y hacer que los programas, datos e información estén disponibles para cualquier elemento de la red que lo solicite, sin importar el lugar físico o localización del recurso. Enfocado en este punto, un aspecto que se ha vuelto imprescindible actualmente es la velocidad con que la que la información puede estar disponible.

Es así, que las investigaciones se han dirigido en cómo mejorar y elevar cada día más la velocidad de transmisión de las redes de comunicación; dando como resultado una nueva generación de redes de alta velocidad, con mucho desarrollo y tecnología de por medio que ha permitido no solo el envío de datos, sino también, de audio, video y contenido multimedia.

Las empresas de hoy, conocedoras de la realidad tecnológica y la necesidad de tener su activo más importante, la información; al alcance en cualquier lugar y momento, se han visto involucradas en los avances que han cambiado completamente la perspectiva del mundo comercial. Es así, que la tecnología de la información ha evolucionado en conjunto con el desarrollo, tanto de las redes de comunicación como de la competitividad empresarial de nuestros tiempos.

Petroindustrial, como filial de Petroecuador, constituye la principal empresa de industrialización del petróleo, refinación y producción de derivados existente en el país, abasteciendo aproximadamente el 80% del consumo interno. Por este motivo y dada su importancia, es una de las empresas que está a la vanguardia en la implementación de los avances tecnológicos dentro de sus redes de comunicación.

Por su estructura organizacional y la ubicación de sus plantas industriales a nivel nacional, tiene la necesidad de disponer de la información de forma rápida y eficiente con el objetivo de consolidarla en la matriz, y permitir de esta forma la

toma de decisiones oportunas frente a los factores que influyen en su funcionamiento.

Vista la importancia que las redes de comunicación tienen actualmente en el desempeño de una empresa, se hace necesario instalar sistemas de administración que permitan manejar de forma óptima los recursos que ésta ofrece a los usuarios, haciéndose necesario, no solo enfocarse en el uso de una herramienta de administración; sino también, en el desarrollo de normas de control que limite el uso indiscriminado de recursos, que en algunos casos son muy necesarios pero que también son limitados.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I

INTRODUCCIÓN A REDES DE ALTA VELOCIDAD

1.1. Redes de alta velocidad.
1.2. Características principales.
1.3. Ventajas y desventajas.
1.4. Aplicaciones generales.

1. INTRODUCCIÓN A REDES DE ALTA VELOCIDAD

Las redes de datos desde su inicio se han convertido en parte fundamental de los actuales sistemas de tecnología de la información; constituyéndose en el pilar principal para el uso compartido de recursos tecnológicos en empresas, grupos gubernamentales, científicos y universitarios.

"La mayoría de las redes fueron instaladas a finales de los años 60 y 70, cuando el diseño de las redes se consideraba la piedra filosofal de la investigación informática y el desarrollo de tecnología de punta; dando como resultado numerosos modelos de redes con diferentes tipos de tecnologías como la de conmutación de paquetes, redes de área local con detección de colisión, redes jerárquicas en empresas, y muchas otras de elevada calidad."[1]

En vista de este avance, a comienzos de los años 70, se consideró la necesidad de estandarizar los protocolos de inter-operatividad de las distintas aplicaciones dentro de la comunicación de red; lo que pronto dio paso a la investigación y desarrollo de un conjunto de protocolos, distribuidos en un conjunto bien definido de capas, de modo que las aplicaciones pudieran comunicarse entre sí, con independencia de la tecnología de red que las soportare y del sistema operativo sobre el que se ejecutaba cada aplicación.

Este avance conlleva al crecimiento de las redes tanto domésticas como de área local y de alta velocidad, que pronto tomaron su espacio dentro de la tecnología de las comunicaciones, como dentro de la vida diaria de las empresas y demás usuarios.

Hoy en día la Tecnología de Transmisión de Información ha tenido un cambio evolutivo y de progreso tan fuerte, que tiene muy pocos campos de la tecnología que lo puedan igualar; y, por ende el aumento de las prestaciones en los sistemas de comunicación es realmente espectacular, lo que ha dado lugar a un sin número de ventajas y desventajas dentro del ámbito de las telecomunicaciones. Los factores claves de este progreso son: [2]

a) El uso universal de tecnología digital en las redes públicas de telecomunicaciones,
b) La consolidación de la Fibra Óptica como medio de transmisión de alta capacidad,

---

[1] Tutorial y descripción técnica de TCP/IP:
http://ditec.um.es/laso/docs/tut-tcpip/3376c11.html. 2000-07-14.
[2] Marzo Lázaro, José Luis. "Control de Tráfico en Redes de Altas Prestaciones":
http://eia.udg.es/~marzo/doctorat/ctav_v00.pdf. Año 2001. Pág. 2.

c) La adopción universal de algunos protocolos (**CSMA/CD**-ethernet, o TCP/IP), en Internet.

En las tablas 1.1 y 1.2 se muestran algunos aspectos importantes acerca de la evolución de las redes, y se hace una pequeña comparación entre las tecnologías para transmisión de datos que han ido evolucionando con el paso de los años. Hay que tomar en cuenta que muchos de estos datos dependen del tipo y topología de red en los que hayan sido recabados.

Detalle	Velocidad estándar	Alta velocidad
Paquetes por segundo	Miles	Millones
Ancho de banda	64 Kbps – 2 Mbps	150 Mbps – 1 Gbps
Asignación de banda	Fija	Dinámica
Tipos de tráfico	Datos (voz)	Multimedia (integración de servicios)
Retardo por conmutación	20-50 ms	10 ms
Retardo por propagación	Insignificante	Significativo
Control de errores	Enlace a enlace	Extremo a extremo
Cuello de botella	Ancho de banda de los enlaces	Capacidad (ancho de banda) de conmutación

Tabla: 1.1 Comparación de la Evolución de las Redes

FUENTE: Marzo Lázaro, José Luis. "Evolución de las Tecnologías y Control de Tráfico": http://eia.udg.es/~marzo/doctorat/1_doctorat_control_trafic.pdf; Año 2005; Pág. 3.

Adentrándonos en los términos técnicos relacionados con las Redes de Alta Velocidad, se puede iniciar diciendo que el término 'alta velocidad' es relativo, dado que en los años 70, una línea de datos dedicada de 4800 bps era considerada de 'muy' alta velocidad. Para el periodo entre el año 2001 - 2005 los enlaces de redes metropolitanas MAN de 2,34 Mbps o superiores, y redes de área local LAN de 10, 100 y 1000 Mbps son normales.[2]

[2] Marzo Lázaro, José Luis. "Control de Tráfico en Redes de Altas Prestaciones": http://eia.udg.es/~marzo/doctorat/ctav_v00.pdf. Año 2001. Pág. 1.

Tecnología	Velocidad	Distancia	Comentarios
CSMA/CD	10-100-1000 Mbps	< 500 m	Bajo rendimiento, barata, simple, descentralizado. Utilización de conmutación de tramas.
FDDI	100 Mbps	< 200 Km	Compleja, mayor carga mayor rendimiento
DQDB	34, 150		Muy compleja, precursora de ATM
X-25	Hasta 64 Kbps	Ilimitada	Lento, funcionalidades obsoletas
Frame Relay	Hasta 2 Mbits	Ilimitada	Simple, tráfico síncrono
ATM	155 Mbps	Ilimitada	Compleja, Overhead fijo, diferentes clases de tráfico.

Tabla: 1.2 Comparación Tecnologías de Transmisión de Datos y su Evolución

FUENTE: Marzo Lázaro, José Luis. "Evolución de las Tecnologías y Control de Tráfico": http://eia.udg.es/~marzo/doctorat/1_doctorat_control_trafic.pdf; Año 2005; Pág. 12.

Por otro lado, los mecanismos de control y gestión de la transmisión de estas redes son incapaces, o cuando menos simplemente ineficientes, para conseguir objetivos similares en redes de mayor velocidad. Aquí es donde aplicaremos el término 'alta velocidad', es decir aquella velocidad para la cual se requieren nuevas técnicas de gestión y control de la red que la soporta.

1.1.REDES DE ALTA VELOCIDAD.

Adentrándonos más en este mundo de las telecomunicaciones hay que hacerse una pregunta muy importante, *¿Por qué redes de alta velocidad?* La siguiente respuesta sería la más simple: *"Porque mediante una sola fibra óptica se pueden transmitir enormes cantidades de información digital a velocidades teóricamente cercanas a los 1,28 terabits (1.200 gigabits) por segundo, asegurando no sólo rapidez, sino que eficiencia en el transporte y entrega final de datos"*. Y todo esto mediante un cable de flexibles filamentos de vidrio (fibra óptica), más delgados que un cabello humano, que al combinarse con el uso de nuevas formas de transmisión permiten calidad de servicio, entre otras propiedades; he aquí el porqué de las redes de alta velocidad.

Se puede enumerar brevemente algunas redes de alta velocidad. Fast and Switched Ethernet, que son variaciones de Ethernet donde se aumenta la velocidad y se incluye la topología en estrella dentro del diseño de redes, pero en cualquier caso, sigue utilizando

el mismo protocolo CSMA/CD para control de tráfico dentro de la red; SMDS (Switched Multimegabit Data Service) es el nombre que reciben las redes públicas especializadas en transporte de datos a media/alta velocidad, pero que no soportan servicios en tiempo real. SONET (Synchronous Optical Network) o Synchronous Digital Hierarchy (SDH), son redes portadoras, que ofrecen servicio a bajo nivel y utilizan fibra óptica y multiplexación digital jerárquica para el enrutamiento de paquetes dentro de su estructura.[2]

1.1.1. **El Problema de la congestión.**

Es difícil definir de manera clara el estado de congestión para un sistema de comunicaciones, pero todos tenemos una idea intuitiva de lo que esto significa. Es por este motivo que este término, congestión, tiene un peso sumamente importante a la hora de tratar con redes de alta velocidad en la transmisión de información.

"La consecuencia de la congestión dentro de un sistema de comunicaciones, es que los paquetes transmitidos aumenten su tiempo de espera en los buffers a expensas de ser retransmitidos, y si la ocupación del buffer supera su propia capacidad, finalmente se pierden paquetes, quedando de esta forma la comunicación y envío de información inconclusa. El resultado final es que el sistema queda plagado de retransmisiones que afectan el flujo efectivo y la eficiencia de la red cae de manera drástica."[2]

Todo esto se resume en tres aspectos: retardo, perdida de paquetes y caída del flujo efectivo. El punto clave es definir a partir de que aspecto se puede decir que una red se encuentra en estado de congestión. El problema en general es que, la degradación de los parámetros mencionados afecta de forma diferente a los usuarios y/o a los servicios que presta una red. Tampoco es fácil determinar el periodo de tiempo en el que definimos la congestión (ms, seg, min, horas, etc.,). La clave está en definir el concepto de 'utilidad' de la red para un usuario; la degradación de está utilidad en términos de máximo retardo, máxima pérdida de paquetes o servicios, ayudan a dar una idea de cuál es la apreciación de un usuario respecto a un sistema de comunicaciones en congestión.

Las redes que incorporan técnicas de control de congestión, lo que intentan son prevenir o reducir en lo posible los efectos de la congestión en la 'utilidad' que percibe el usuario por los servicios que utiliza.

---

[2] Marzo Lázaro, José Luis. "Control de Tráfico en Redes de Altas Prestaciones": http://eia.udg.es/~marzo/doctorat/ctav_v00.pdf. Año 2001. Pág. 13.

1.2.CARACTERÍSTICAS PRINCIPALES.

Como se ha explicado desde un inicio, las redes de alta velocidad se están convirtiendo en una tendencia tecnológica, a la que todas las empresas y entidades que hacen uso de las redes de información para mejorar su desempeño van a llegar; y dado este efecto es que se hace necesario explicar las principales características que incorpora esta nueva tecnología.

1.2.1. **Algoritmos de Enrutamiento.**

Dentro de la arquitectura de una red de datos, la capa de Red, (Capa 2 - OSI), es la encargada de llevar los paquetes de datos desde el origen (estación transmisora) hasta el destino (estación receptora). Para asegurar que un paquete de datos llegue a su destino completo y a tiempo, puede requerir que el algoritmo de ruteo encargado de escoger las rutas y las estructuras de datos, cumpla con ciertas propiedades que aseguren la eficiencia de su trabajo.

"Las propiedades que debe cumplir un algoritmo de ruteo son: corrección, estabilidad, robustez, equitatividad, sencillez y optimalidad."[3]

- Corrección.- Que sea capaz de corregir errores,
- Sencillez.- Que no sea de difícil implementación,
- Robustez.- Que funcione dentro de la red por años, sin fallas generales y que esté preparado para manejar cambios de topología y tráfico, sin requerir el aborto de las actividades o el reinicio de la red.
- Equitatividad y la Optimalidad.- Ser Equitativo y óptimo en la operación.

Algo que debe caracterizar a un algoritmo de ruteo debe ser el minimizar el retardo de los paquetes, disminuyendo escalas y ancho de banda por un lado y por el otro, el maximizar el rendimiento total de la red para brindar un óptimo desempeño.

Dentro del sistema OSI, la capa de Red (Capa 2) es la encargada de proporcionar la dirección lógica, que permite que dos sistemas dispares que se encuentran en redes lógicas diferentes determinen una posible ruta para comunicarse e intercambiar información. En la capa de red es donde residen y operan los algoritmos que implementan los protocolos de enrutamiento; y por lo tanto, se convierten en parte del software de la

[3] Goitia, María Julieta. "Protocolos de Enrutamiento para la Capa de Red en Arquitecturas de Redes de Datos": http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/ProtocolosRed.PDF. Año 2002.

capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de información.

1.2.2. **Clasificación de los Algoritmos de Enrutamiento.**

Los Algoritmos de Enrutamiento se clasifican de la siguiente manera:

- ***Algoritmos Estáticos ó No Adaptables.-*** Son algoritmos que no basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico ni en la topología, es decir, que las rutas para ir de un nodo a otro nodo están calculadas por adelantado y se cargan en cada ruteador al iniciar la red. La principal desventaja de este tipo de algoritmos, es que no pueden responder a situaciones cambiantes como saturación del canal, exceso de tráfico o fallo de una línea o enlace.[3]

  Entre los algoritmos estáticos tenemos los siguientes tipos:

  - *Enrutamiento por Trayectoria más Corta*.- Es una técnica sencilla y fácil de entender e implementar por lo que tiene un amplio uso. Consiste en armar un grafo de la red, donde cada nodo representa un ruteador y cada arco del grafo representa una línea de comunicación o enlace. Así el algoritmo elige la ruta más corta entre los nodos basándose en la información del grafo que posee y la longitud o peso que se ha calculado para esa ruta.

  - *Enrutamiento por Inundación*.- Esta técnica consiste en enviar cada paquete de entrada por todas las rutas de salida, excepto por la que llego. Este proceso genera gran cantidad de paquetes duplicados, de hecho una cantidad infinita a menos que se tome algún correctivo para detener este proceso que origina consumo indebido de recursos de la red.

  - *Enrutamiento basado en Flujo*.- Está técnica no solo usa la topología de la red para el enrutamiento, sino también la carga de tráfico de cada línea de comunicación. Este análisis se basa en que para una línea dada, si se conoce la capacidad y el flujo promedio, es posible calcular el retardo promedio de los paquetes en esa línea utilizando la teoría de colas. Al tener el retardo

[3] Goitia, María Julieta. "Protocolos de Enrutamiento para la Capa de Red en Arquitecturas de Redes de Datos": http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/ProtocolosRed.PDF. Año 2002.

promedio de todas las líneas, es fácil conocer el retardo promedio de un paquete en toda la subred.

Así, el problema de enrutamiento se reduce a encontrar un algoritmo que produzca el retardo promedio mínimo de la subred. Pero para el uso de esta técnica es necesario conocer por adelantado la topología de la red, la matriz de tráfico y por último la matriz de capacidad.

- ***Algoritmos Dinámicos ó Adaptables.-*** Son algoritmos que cambian sus decisiones de enrutamiento para reflejar o adaptarse a los cambios de topología o tráfico que se presenten dentro de la red. La información de ruteo la obtienen de sus nodos o ruteadores vecinos y se basan en el cambio de rutas, y métricas usadas para medir el peso del enlace en la red. Este tipo de algoritmos no pueden ser demasiado complejos ya que son implementados en los ruteadores y deben ejecutarse en tiempo real con recursos de CPU y memoria que dispone el ruteador.[4]

  Entre los algoritmos Dinámicos tenemos los siguientes tipos:

  - *Enrutamiento Vector Distancia*.- Este tipo de algoritmo opera haciendo que cada ruteador coopere en el cálculo distribuido de las rutas hacia todos y cada uno de los destinos de la red; es decir, que cada ruteador calcula el mejor camino (mínimo coste) a todos los destinos y luego da a conocer a todos sus vecinos la tabla de rutas que ha calculado. Figura 1.1.

    La información que comunica cada ruteador, contendrá la dirección o vector y el coste o distancia a cada destino. Una vez que el ruteador analiza las rutas anunciadas por sus vecinos puede calcular un mejor camino hacia un destino. Este algoritmo tras varias iteraciones converge a los mejores caminos estabilizando las rutas. Una característica de este algoritmo es que el cálculo de las rutas en simple, asíncrono, incremental y distribuido. Algunos ejemplos de protocolos que utilizan este tipo de algoritmos son: RIP, IPX-RIP, DECnet, IGRP, EIGRP.[5]

[4] Muratori, Uzuri. "Tipos de Protocolos de Enrutamiento": http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-TiposRouting.pdf. Año 2002 Pág. 3
[5] TCP/IP Tutorial and Technical Overview: http://ditec.um.es/laso/docs/tut-tcpip/3376c33.html#vda. 2005-10-12.

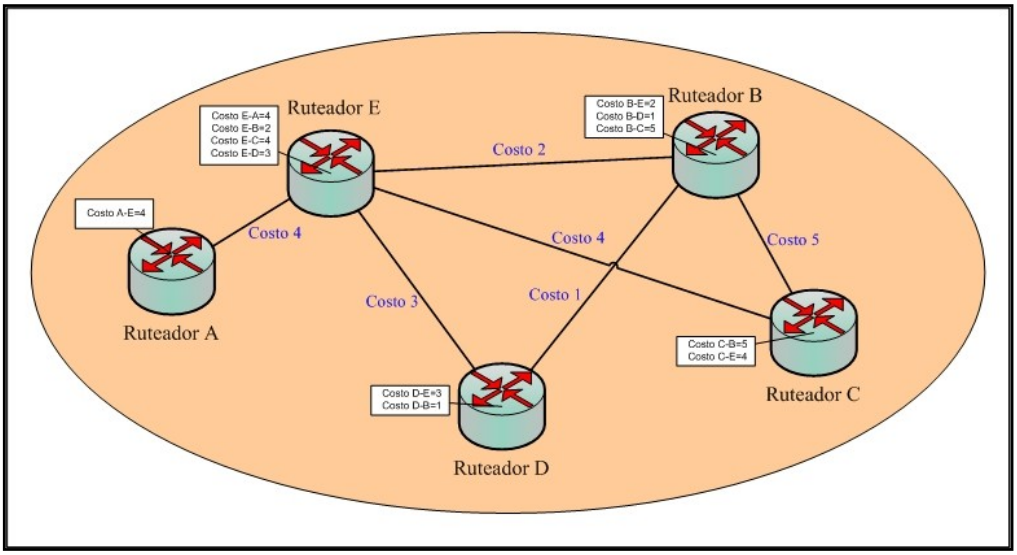


Fig: 1.1: Enrutamiento Vector-Distancia
FUENTE: Propio

- *Enrutamiento por Estado de Enlace*.- Este algoritmo se aproxima a una base de datos distribuida replicada y no a un cálculo distribuido incremental de rutas; es así, que cada ruteador posee información global de la red, nodos y enlaces; la cual fue obtenida enviando paquetes de prueba ECHO para verificar si un nodo es alcanzable y el coste de dicha ruta hasta ese nodo. Figura 1.2.

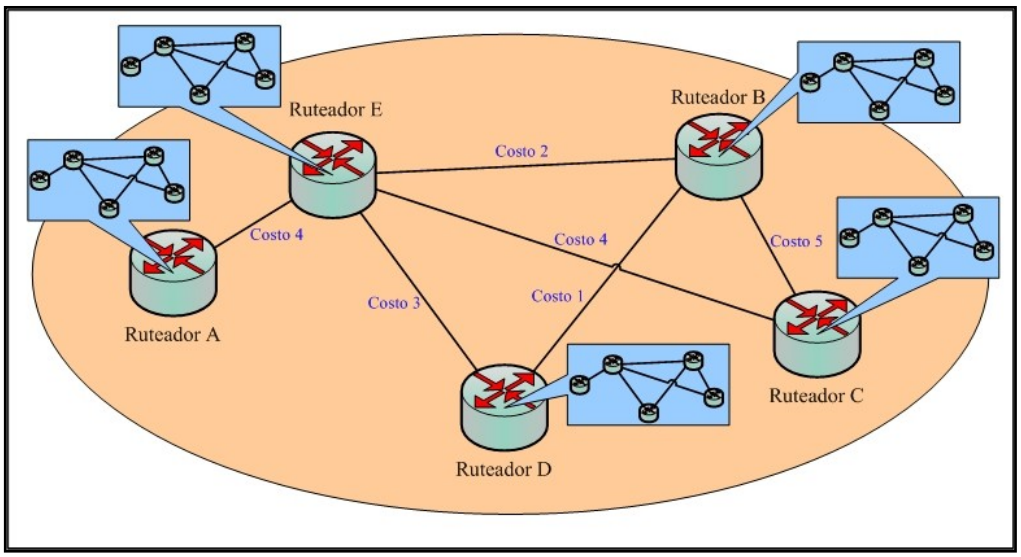


Fig: 1.2: Enrutamiento Estado de Enlace
FUENTE: Propio

Una vez obtenida toda la información de la red, esta es distribuida a redes activas y con ruteadores vecinos. La distribución de la información de ruteo

se la realiza inundando toda la red para que llegue a todos los ruteadores. Cuando la información ha llegado a todos los ruteadores, todos tiene la misma imagen (grafo) de toda la red, de ahí es de donde eligen las mejores rutas. Por esto, este algoritmo tiene mejor tiempo de convergencia que el Vector-Distancia ante cambios de la red. OSPF, IS-IS, PNNI son algunos protocolos que utilizan este algoritmo en su estructura de enrutamiento.

- *Enrutamiento Vector de Dirección o Híbridos-Equilibrados*.- Este algoritmo es similar al de Vector Distancia, donde el cálculo de las rutas es distribuido, es decir que cada ruteador realiza su propio cálculo de las rutas o caminos. Es una mezcla entre los algoritmo de Vector Distancia y Estado de Enlace. La información que los ruteadores entregan a sus vecinos incluye no solo las rutas calculas, sino también todo el camino (path) hasta el destino de cada ruta. [6] Figura 1.3.

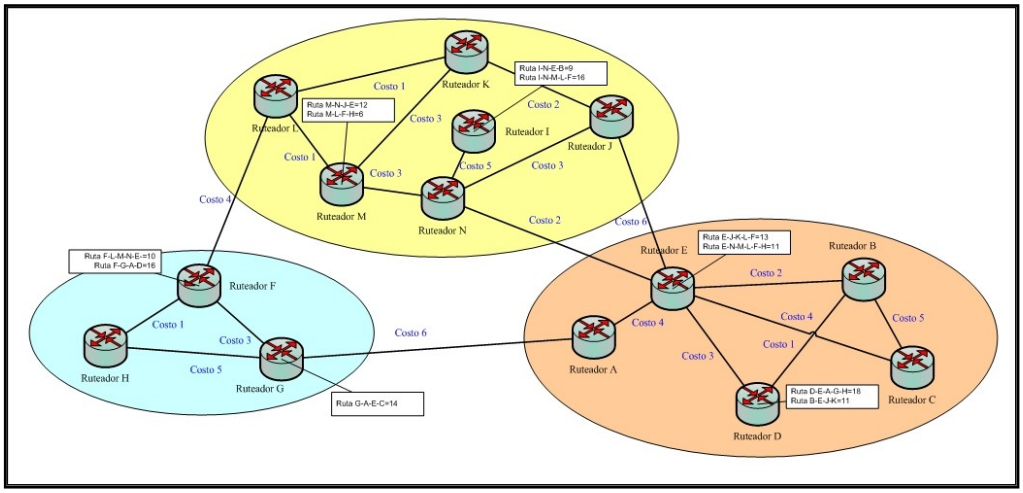


Fig: 1.3: Enrutamiento Vector de Dirección
FUENTE: Propio

Un ejemplo de protocolo que utiliza este tipo de algoritmos de enrutamiento en su estructura es el protocolo BGP.

- *Enrutamiento jerárquico*.- A medida que el tamaño de las redes se incrementa, también se incrementan proporcionalmente las tablas de enrutamiento dentro del ruteador. Dado el crecimiento de las tablas, estas no solo consumen memoria del ruteador, sino que también necesitan más tiempo de CPU para examinarlas y más ancho de banda para enviar informes de estado y rutas entre ruteadores. En cierto momento, la red puede crecer hasta

[6] Interconecting Cisco Network Devices, Vol.1 version 2.3 Student Guide ICND 2.3. Año 2006; Pág. 3-28.

el punto, en que ya no es conveniente tener en cada ruteador una entrada en la tabla de ruteo para cada uno de los demás ruteadores que componen la red, por lo que el enrutamiento tendrá que hacerse jerárquicamente, como ocurre en la red telefónica[7]. Figura 1.4.

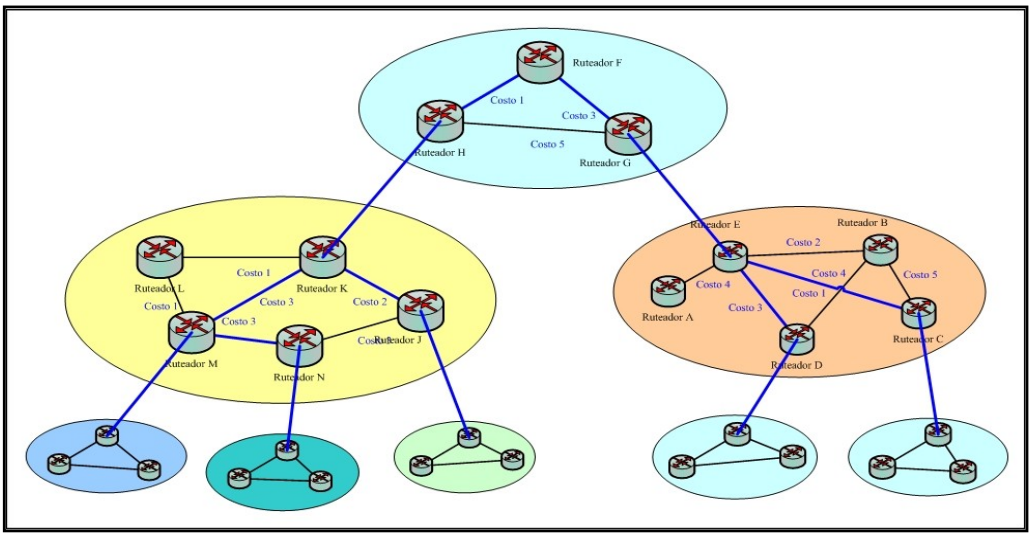


Fig: 1.4: Enrutamiento Jerárquico
FUENTE: Propio

Al emplearse enrutamiento jerárquico, los ruteadores se dividen en lo que llamamos regiones, en donde cada ruteador conoce todos los detalles para enrutar un paquete dentro de su región, pero desconoce la estructura interna manejada en otras regiones. Al interconectar diferentes redes, es natural considerar a cada una como región independiente, a fin de liberar a los ruteadores de la necesidad de conocer la estructura topológica de las demás.

1.2.3. **Métricas de Enrutamiento.**

Dentro de todo el contexto de ruteo, hay que analizar las diferentes métricas usadas por los algoritmos de enrutamiento y de switching para determinar la mejor ruta, basándose en la información que contiene su tabla de ruteo. Los sofisticados algoritmos de ruteo pueden basar su selección en múltiples métricas, combinándolas en una sola métrica (híbrida). A continuación se describen las métricas más usadas: [8]

[7] Routing Basics. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm. 2006-10-12.

- ***Longitud de Ruta (Path length)***.- Es la más común de las métricas de enrutamiento. Algunos protocolos de enrutamiento permiten que los administradores de la red atribuyan costos arbitrarios a cada enlace de la red. En este caso la longitud de la ruta es la suma de los costos asociados de cada enlace atravesado. Otros protocolos de enrutamiento definen el conteo de saltos; esta métrica especifica el número de pases a través de productos de internet working, tal como ruteadores, que un paquete debe tomar en la ruta de un origen a un destino.

- ***Confiabilidad (Reliability)***.- En el contexto de los algoritmos de ruteo, hace referencia a la confiabilidad por lo general descrita en términos de costo de bit-error para cada enlace de red. Cuando se presenta una falla en la red, ciertos enlaces de la misma podrían ser reparados más fácilmente o más rápidamente que otros. Cualquier factor de confiabilidad puede ser tenido en cuenta en la asignación de las clasificaciones de confiabilidad; estos valores numéricos y arbitrarios son atribuidos a los enlaces por el administrador de la red generalmente.

- ***Retardo (Routing delay)***.- El retardo de enrutamiento se refiere a la longitud del tiempo requerido para mover un paquete desde el lugar de origen hacia su destino a través de la red. El retardo depende de muchos factores incluyendo el ancho de banda de enlaces de la red intermedios. Las colas en los puertos de cada ruteador a lo largo del camino; la congestión en todos los enlaces de red intermedios y la distancia física que tiene que recorrer un paquete. Porque el retardo es un conglomerado de algunas variables importantes, es una métrica común y útil.

- ***Ancho de Banda (Bandwidth)***.- El Ancho de Banda se refiere a la capacidad de tráfico disponible de un enlace. En igualdad de circunstancias, un enlace de Ethernet de 10 Mbps sería preferible a una línea arrendada de 64 kbps. Aunque el ancho de banda es una clasificación de rendimiento máximo alcanzable sobre un enlace. Las rutas a través de enlaces con mayor ancho de banda no necesariamente proveen mejores rutas que las rutas a través de enlaces más lentos. Por ejemplo, si un enlace rápido está ocupado, el tiempo actual requerido para enviar un paquete a su destino podría ser mayor.

- ***Carga (Load)***.- La carga se refiere a que tipo de red o recurso de red, por ejemplo si un enrutador está ocupado, la carga puede ser calculada en varias formas, incluyendo la utilización del CPU y los paquetes procesados por segundo. Monitorear estos parámetros continuamente dentro de un recurso de red puede provocar más carga para sí mismo.

- ***Costo de comunicación (Communication cost)***.- El costo de comunicación es otra importante métrica, sobre todo porque algunas empresas no se preocupan por el rendimiento tanto como se preocupan por los gastos de operaciones. Aunque la demora en línea puede ser más larga, ellos enviarán paquetes sobre sus propias líneas que por las líneas públicas que cuestan dinero durante el tiempo de uso del enlace.

1.2.4. **Protocolos de Enrutamiento.**[8]

Dentro de las características nuevas que presentan las redes de alta velocidad, una muy relevante y de vital importancia son los protocolos de enrutamiento que se manejan para el direccionamiento de los paquetes que transmiten a través de una red de información, ya que al ser la congestión, una de las principales causas de las caídas del rendimiento de las redes, se hace necesario administrar y controlar de mejor manera el flujo de paquetes que tratan de acceder a un canal o enlace de transmisión.

Hay que tomar muy en cuenta, que los protocolos enrutados son transportados a través de una red, por los protocolos de enrutamiento. En este contexto, los protocolos enrutados, se refiere a los todos los protocolos de red los cuales realizan una variedad de funciones requeridas para la comunicación entre las aplicaciones usuario y los dispositivos de destino; estas funciones pueden diferir ampliamente entre los paquetes de protocolos.

La confusión entre los términos protocolo enrutado y protocolos de enrutamiento es muy común. Entre los protocolos enrutados tenemos: Internet Protocol (IP), DECnet, AppleTalk, Novell NetWare, OSI, Banyan VINES, and Xerox Network System (XNS). Por otro lado, los protocolos de enrutamiento son aquellos que implementan algoritmos de enrutamiento. Dicho en otras palabras, los protocolos de enrutamiento son usados por los sistemas intermedios para construir las tablas, que se utilizan para determinar las direcciones y seleccionar las mejores rutas para los protocolos enrutados. Dentro de los protocolos de enrutamiento tenemos: Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Routing Information Protocol (RIP).

---

[8] Muratori, Uzuri. "Características del Enrutamiento Dinámico en Internet": http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-Routing.pdf. Año 2005.

Así, los protocolos de enrutamiento utilizan o basan su estructura como tal en los algoritmos de enrutamiento anteriormente descritos, con el único fin de proporcionar el mejor rendimiento y operatividad a la red al momento de encaminar por la mejor ruta, los paquetes de datos que lleguen hasta un equipo destinado para tal propósito.

Dentro de una Intranet estática y pequeña, las tablas de enrutamiento se pueden crear y mantener manualmente. Pero a medida que la Intranet va creciendo como es el caso de Internet, muchas empresas y organizaciones, los ruteadores mantienen sus propias tablas actualizadas, intercambiando información unos con otros de forma automática y dinámica. Los ruteadores son capaces de descubrir dinámicamente, si se ha añadido una nueva red; que el camino a un destino ha fallado y que ya no es posible alcanzar dicho destino ó que se ha añadido un nuevo ruteador a la WAN.[9]

No existe una única norma para el intercambio de información entre ruteadores y dada esta libertad de elección del protocolo, ha estimulado la competencia y mejora de estos protocolos dedicados a este trabajo. Dentro de una organización, las funciones manejo y control de Red se denominan un Sistema Autónomo (AS Autonomous System); por lo que se puede elegir por el protocolo de enrutamiento más apropiado y acorde a las necesidades de su red.

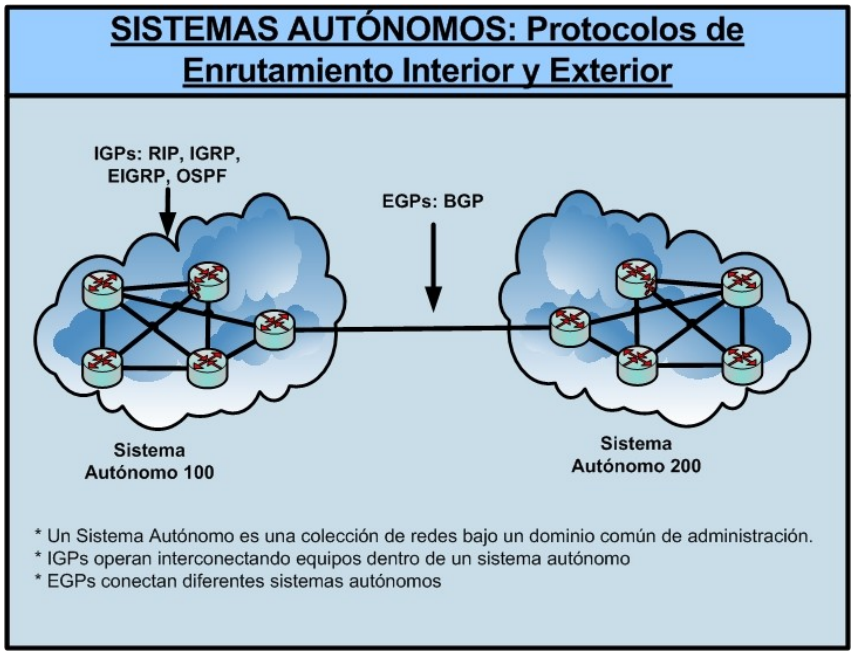


Fig: 1.5: Clasificación de Protocolos de Enrutamiento
FUENTE: Propio

[9] Marzo Lázaro, José Luis. "Evolución de las Tecnologías y Control de Tráfico": http://eia.udg.es/~marzo/doctorat/1_doctorat_control_trafic.pdf; Año 2005; Pág. 12.

Iniciando con el abuelo de las redes, ARPANET[10] y dado que su estructura manejaba el concepto de AS, que eran una colección de redes manejadas por una solo entidad de control, se debe notar que manejaba 2 tipos de protocolos, el primero denominado IGP *("Interior Gateway Protocol")*, que se utilizaba para comunicar 2 ruteadores dentro del mismo AS o Intra-AS y el segundo llamado EGP *("Exterior Gateway Protocol")* que era utilizado para comunicar ruteadores de distintos AS o Inter-AS.

El Protocolo de Información de Enrutamiento RIP *("Routing Information Protocol")* es un estándar muy usado dentro de los IGP. RIP es muy popular por su sencillez y su gran disponibilidad. Sin embargo, el nuevo protocolo OSPF *("Open Shortest Path First")* Abrir Primero el Camino más Corto, dispone de un conjunto más rico de funciones que posibilitan el enrutamiento en redes mucho más grandes donde RIP no es eficiente.

1.2.5. **Interior Gateway Routing Protocol (IGRP)** [11]

Este protocolo de enrutamiento fue desarrollado a mediados de los 80 por Cisco System In. El principal objetivo de Cisco, fue proveer un protocolo robusto para el enrutamiento dentro de los Sistemas Autónomos. En esta época, el protocolo más popularmente usado para el enrutamiento de información dentro de redes de pequeño y mediano tamaño relativamente homogéneas era Routing Information Protocol RIP, pero sus limitaciones aparecieron junto con el crecimiento de las redes.

La popularidad de los ruteadores Cisco y la robustez de IGRP, animaron a muchas organizaciones a reemplazar el RIP con IGRP en las redes de mayor tamaño donde RIP no era eficiente.

IGRP es un Interior-Gateway Protocol (IGP) que trabaja con vector de distancia. El protocolo de enrutamiento Vector-Distancia, compara matemáticamente las rutas usando alguna medida de distancia. Los ruteadores usan el protocolo Vector-Distancia, para enviar toda o una porción de su tabla de enrutamiento en mensajes de actualización a intervalos regulares a todos sus vecinos ruteadores. Como esta información se prolifera a través de la red, los ruteadores pueden identificar nuevos destinos adheridos, conocer sobre las anomalías dentro de la misma y lo más importante, recalcular las distancias hacia destinos conocidos.

---

[10] TCP/IP Tutorial and Technical Overview:
http://ditec.um.es/laso/docs/tut-tcpip/3376c12.html#arpanet. 2000-07-14.
[11] Interior Gateway Routing Protocol (IGRP). Cisco Documentation:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm. 2006-09-13.

IGRP usa combinaciones de métricas como Retardo de la Red, Ancho de Banda, Confiabilidad y Carga para realizar los cálculos y seleccionar la mejor ruta. Los administradores de red pueden colocar un factor de peso para cada una de esas métricas, permitiendo flexibilidad en el manejo de la red. IGRP usa los pesos colocados por el administrador o los de default, para automáticamente calcular las rutas óptimas. Además provee un fino rango para sus métricas, lo cual permite mediciones satisfactorias en redes con pequeñas variaciones en sus características de desempeño y dado que los componentes de las métricas son combinadas en algoritmos definidos por el usuario, el resultado es que el administrador puede tener influencia en la selección de rutas en una manera intuitiva.

IGRP proporciona una flexibilidad adicional, ya que permite enrutamiento multicamino (multipath), lo que ayuda, cuando una de las líneas de enlace se cae y habilita que la transmisión de paquetes se realice por la ruta alterna. IGRP provee un número de características que son diseñadas para incrementar su estabilidad. Estas son: *holddowns, split horizons y poison reverse updates*.

Holddowns es usado para prevenir mensajes de actualización inapropiados o incorrectos, que suceden cuando un ruteador se cae y los demás tardan mucho tiempo en enterarse, lo que puede provocar pérdida de paquetes en la transmisión. De esta forma, se incrementa los tiempos de envió de actualizaciones permitiendo a todos los ruteadores de una red conocer cuando un vecino esta fuera de alcance.

Split Horizons deriva del hecho de que nunca es útil mandar información sobre la misma ruta por la cual ingreso. Esta regla ayuda a prevenir lazos de enrutamiento y proporciona a IGRP mayor estabilidad.

Poison Reverse Update, a diferencia de Split Horizons que está preparado prevenir lazos entre ruteadores adyacentes; está destinado para evitar y romper lazos de enrutamiento más grandes. El incremento en las métricas de enrutamiento generalmente indica lazos. Poison reverse updates permite remover la ruta de un lazo grande y colocarlo en hold-down.

1.2.6. **Enhanced Interior Gateway Routing Protocol (E-IGRP)**[12]

EIGRP es la evolución de su predecesor IGRP, y es un protocolo de enrutamiento híbrido, propietario de Cisco Systems In, que ofrece lo mejor de los algoritmos de Vector-Distancias y Estado Enlace. Esta evolución es el resultado de los cambios y las diversas demandas presentados en los sistemas de red a gran escala. Se considera un protocolo sumamente avanzado, que se basa en las características normalmente asociadas con los protocolos de Estado-Enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Sin embargo, EIGRP es más fácil de configurar que OSPF. También mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una mejor arquitectura y pueda mantener las inversiones actuales en IGRP.

Los ruteadores EIGRP, mantienen información de ruta y topología a disposición en la memoria RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos. Las rutas reciben un estado y se pueden rotular para proporcionar información adicional de utilidad. EIGRP se apoya en 4 fundamentales conceptos: Tabla de Vecinos, Tabla de Topología, Estados de Ruta y Etiquetas de Ruta.

- ***Tabla de vecinos***.- Cada ruteador EIGRP mantiene una tabla de vecinos que enumera a los ruteadores adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP. Cuando un ruteador descubre a un nuevo vecino, su dirección e interfaz son insertadas en la tabla de vecinos de forma que es registrado como un nuevo elemento de la red.

- ***Tabla de topología***.- La tabla de topología se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos. EIGRP toma la información proporcionada en la tabla de vecinos y la tabla de topología para calcular las rutas de menor costo hacia cada destino. EIGRP rastrea esta información para que los ruteadores puedan identificar y conmutar a rutas alternativas rápidamente.

  La información que el ruteador recibe de los vecinos, se emplea para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los ruteadores EIGRP mantienen una tabla de topología por cada protocolo

[12] Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm. 2007-02-01.

configurado de red (como IP, IPv6 o IPX). La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

- ***Estado de Ruta***.- Cada destino ingresado en la tabla de topología puede existir en dos estados: Activo y Pasivo. Un destino se encuentra en estado pasivo cuando el ruteador no ejecuta un nuevo cómputo, y se encuentra en estado activo cuando el ruteador si realiza un nuevo cómputo. Un nuevo cómputo ocurre cuando un destino no tiene ningún sucesor viable. Mientras un destino esté en estado activo, un ruteador no puede cambiar la información de los destinos en la tabla de rutas. Después de que un ruteador ha recibido de sus vecinos la información de que ha acabado un nuevo computo, las entradas para los destinos en la tabla de topología regresan al estado pasivo y el ruteador puede seleccionar a un sucesor.

- ***Etiquetas de Ruta***.- EIGRP soporta rutas internas y externas. Las rutas internas se originan dentro de uno AS de EIGRP. Por lo tanto, una red directamente conectada y configurada para operar EIGRP es considerada una ruta interna y es propagado con esta información en todo el AS. Las rutas externas son aprendidas por otro protocolo de direccionamiento o residen en la tabla de ruteo como rutas estáticas. Estas rutas son etiquetadas por separado con la identidad de su origen.

  Las rutas externas son etiquetadas con la siguiente información:

  - ID del ruteador EIGRP que redistribuyó la ruta.
  - Número del Sistemas Autónomo de destino.
  - Etiqueta configurable del administrador.
  - ID del protocolo externo.
  - Métrica del protocolo externo.
  - Bit de bandera para enrutamiento default.

  Etiquetar las rutas permite que el administrador de la red personalice el enrutamiento y mantenga flexibles las políticas de control. Etiquetar las rutas es particularmente útil para los Sistemas Autónomos, donde EIGRP interactúa con los protocolos de direccionamiento entre dominios que implementan políticas más globales, resultando en un direccionamiento muy escalable y basado en políticas de ruteo.

1.2.7. **Open Shortest Path First (OSPF)** [13]

[13] Open Shortest Path First (OSPF). Cisco Documentation:

Este protocolo de enrutamiento, fue desarrollado para redes Internet Protocol (IP) por el grupo de trabajo de Interior Gateway Protocol (IGP) de la Internet Engineering Task Force (IETF). Este grupo de trabajo fue formado en 1988 para diseñar un IGP basado en el algoritmo de Shortest Path First SPF (primero el camino más corto) para uso en Internet. Así como el protocolo IGRP, OSPF fue creado debido a que RIP era incapaz de soportar los niveles de exigencia de las nuevas redes más grandes y heterogéneas.

OSPF se derivada de varios esfuerzos de investigación, incluyendo los siguientes: El algoritmo SPF de Bolt, Beranek, y Newman (BBN) desarrollado por ARPANET en 1987. La investigación del Dr. Perlman's de tolerancia a fallos transmisión de información de enrutamiento en 1988. Trabajos de BBN en el área de enrutamiento en 1986 y en una versión temprana del protocolo Intermediate System-to-Intermediate System (IS-IS) de OSI.

Este algoritmo de enrutamiento tiene dos características primarias. La primera, es que figura como un protocolo abierto, lo que significa que su especificación es de dominio público. La especificación de OSPF esta publicada en el RFC 1247. La segunda característica principal es, que está basado en el algoritmo SPF, el cual algunas veces hace referencia al algoritmo de Dijkstra. OSPF contrasta con RIP e IGRP, ya que es un protocolo de enrutamiento Estado de Enlace; es decir, que envía un anuncio de estado de enlace (LSA) a todos los otros ruteadores dentro de la misma área jerárquica, información de interfaces adheridas, métricas usadas, y otras variables son incluidas en los LSA de OSPF. Los ruteadores OSPF acumulan información de los estados de enlace, utilizan el algoritmo SPF para calcular el camino más corto a cada nodo.

A diferencia de RIP, OSPF puede operar dentro de una jerarquía. La entidad más grande dentro de la jerarquía es el Sistema Autónomo (SA). Un Sistema Autónomo es una colección de redes bajo una administración común, compartiendo una misma estrategia de enrutamiento. OSPF es un protocolo Intra-SA (gateway interior), aunque es capaz de recibir y enviar paquetes por otras rutas a otros SAs. Una Base de Datos topológica, es esencialmente un dibujo total de la red en interrelación con los ruteadores. La topología de un área es invisible para las entidades fuera de ésta y al guardar los ruteadores las topologías de áreas separadas, OSPF genera menos tráfico de enrutamiento que si el Sistemas Autónomo no estuviera particionado. Dentro de las áreas de jerarquía se genera un backbone de enrutamiento OSPF, que es el encargado de direccionar los paquetes de información entre los ruteadores adecuados.

---

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm 2006-09-12.

OSPF incorpora características adicionales como igualdad de costo, enrutamiento multicamino y enrutamiento de peticiones de tipo de servicio basado en capas superiores. El enrutamiento basado en tipo de servicio (TOS) soporta aquellos protocolos de capa superior que pueden especificar los tipos particulares de servicio. Por ejemplo, una aplicación podría especificar que cierto dato es urgente. Si OSPF tiene enlaces de alta prioridad a su disposición, este puede ser usado para transportar el datagrama urgente.

OSPF soporta una o más métricas. Si solo una métrica es usada, es considerada arbitraria, y TOS no es soportado. Si más de una métrica es usada, TOS es opcionalmente soportada, a través del uso de una métrica separada (usa una tabla de enrutamiento separada) para cada uno de sus ocho combinaciones creadas por los tres bits de TOS IP (los bits de retardo, rendimiento y confiabilidad). Por ejemplo, si el bit del TOS IP especifica bajo retardo, bajo rendimiento y alta confiabilidad, OSPF calcula rutas para todos los destinos basados en designación de TOS.

Mascaras de subredes IP son incluidas con cada destino anunciado, habilitando mascaras de subredes de longitud variable. Con mascaras de subredes de longitud variable, un red IP puede ser particionada en varias subredes de varios tamaños. Esto provee a los administradores flexibilidad extra en la configuración de las redes.

1.2.8. **Exterior Gateway Protocol (EGP)**[14]

EGP es un protocolo de enrutamiento interdominio muy usado en Internet y además el primero en adquirir aceptación general en Internet, prestó un propósito muy significativo; pero desafortunadamente la debilidad de EGP se ha hecho más aparente a medida que la red de Internet fue creciendo y madurando. Debido a esto, EGP está actualmente siendo reemplazado por protocolos como Border Gateway Protocol (BGP) e Interdomain Routing Protocol (IDRP).

EGP fue originalmente diseñado para permitir la comunicación entre los ruteadores núcleo de Advanced Research Projects Network (ARPANET). La información fue pasada de un nodo fuente individual en distintos dominios administrativos de Internet llamados Sistemas Autónomos hasta el núcleo de los ruteadores, el cual se encargaba de pasar la información a través de la estructura hacia la red del destino de algún otro SA. Es decir, que se generaba un backbone de ruteadores para el enrutamiento de paquetes dentro de la red.

---

[14] TCP/IP Tutorial and Technical Overview. EGP: http://ditec.um.es/laso/docs/tut-tcpip/3376c34.html#erp. 2000-07-14.

Aunque es un protocolo de enrutamiento dinámico, usa un diseño muy simple; no utiliza métricas por lo que no toma decisiones inteligentes. Sus actualizaciones de enrutamiento contienen información de las redes alcanzables a través de los nodos. EGP tiene tres funciones principales. Primero, los ruteadores que manejan EGP establecen un conjunto de vecinos, los cuales son simplemente ruteadores con los que desea compartir información de alcanzabilidad. Segundo, hacen un tipo de encuesta para ver si sus vecinos están vivos y alcanzables. Tercero, mandan mensajes de actualización que contienen información sobre la alcanzabilidad de redes dentro de su SA.

1.2.9. **Border Gateway Protocol (BGP)**[15]

BGP es un protocolo de enrutamiento usado entre Sistemas Autónomos (SA) para intercambiar información de ruteo para Internet, y es comúnmente usado entre los proveedores de Servicios de Internet. (ISP). Cuando BGP es usado entre Sistemas Autónomos, se hace referencia al protocolo como External BGP (EBGP). Si un proveedor de servicios, usa BGP para intercambiar rutas dentro de un SA, entonces se hace referencia al protocolo como Interior BGP (IBGP). A diferencia de otros protocolos de enrutamiento que se comunican mediante paquetes o datos, BGP está orientado a conexión y utiliza TCP como protocolo de transporte.

BGP es un protocolo de enrutamiento muy robusto y escalable, demostrado por el hecho de que es el más empleado en Internet para intercambio de información entre ISP's. Para lograr escalabilidad a este nivel, BGP utiliza muchos parámetros de ruteo y llamadas de atributos para definir las políticas y mantener un ambiente estable de enrutamiento. Un ejemplo de estos atributos es Classless Interdomain Routing (CIDR), que es usado por BGP para reducir el tamaño de las tablas de enrutamiento en Internet. Los vecinos BGP intercambian toda la información de ruteo cuando la conexión TCP a través de sus vecinos ha sido establecida. Cuando son detectados cambios en la tabla de ruteo, los ruteadores BGP envían hacia sus vecinos solamente las rutas que han cambiado; es decir que no envía actualizaciones periódicas y las que son anunciadas indican solamente una ruta óptima hacia un destino.

Las rutas aprendidas vía BGP, han asociado las propiedades que son usadas para determinar la mejor ruta hacia un destino especial cuando existen múltiples rutas para

[15] Border Gateway Protocol (BGP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm. 2006-09-12.

alcanzarlo. Estas propiedades, hacen referencia a los atributos de BGP y su influencia para diseñar una red robusta. A continuación tenemos los atributos principales de BGP:

Atributo Peso.- El peso es un atributo definido por Cisco como local en un ruteador, por lo que no es comunicado a los ruteadores vecinos. Si un ruteador aprende mas acera de la ruta hacia un mismo destino, la ruta con el peso más alto será preferida a la hora del enrutamiento.

Atributo de Preferencia Local.- Este atributo es usado para establecer un punto de salida de un sistema autónomo para una ruta específica y a diferencia del atributo de peso, este es propagado localmente dentro del sistema autónomo.

Atributo Discriminador Multi-salida.- Llamado también Atributo Métrica, es usado como sugerencia para la enrutar hacia otros SA externos, dado que estos pueden estar usando otros atributos BGP para seleccionar la ruta apropiada.

Atributo de Origen.- Indica como BGP aprende acerca de una ruta en particular y puede tener uno de tres posibles valores: IGP: La ruta es interior para el SA original; EGP: La ruta es aprendida vía EBGP; Incompleta: el origen de la ruta es desconocido y es aprendido por otros caminos, esto ocurre cuando la ruta es redistribuida dentro de BGP.

Atributo Ruta Sistema Autónomo.- Cuando una ruta anuncia paso a través de un sistema autónomo, el número del SA es agregado en orden a la lista SA que tiene que atravesar.

Atributo Next-Hop.- El atributo Nex-Hop de EBGP es la dirección IP usada para alcanzar al ruteador anunciado, es decir es el vecino más cercano en una ruta

Atributo Comunidad.- Este atributo proporciona una forma de agrupar los destinos, llamada comunidades a las que las decisiones de direccionamiento como aceptación, preferencia y redistribución se pueden aplicar. Los mapas de rutas son usados para fijar el atributo comunidad. Los atributos de comunidad predefinidos son: NO-Export: No anuncie esta ruta a pares de EBGP; NO-Advertise: No anuncie esta ruta a ningún par; Internet: Anuncie esta ruta a la comunidad de Internet.

1.2.10. **Intermediate System-to-Intermediate System (IS-IS)**[16]

[16] IS-IS - Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/IS-IS. 2006-05-12.

Es un protocolo Estado-Enlace/IGP desarrollado originalmente para enrutamiento de paquetes por ISO/CLNP (International Organization for Standardization/Connectionless Network Protocol). En terminología ISO, un ruteador es referido como un Sistema Intermedio IS. IS-IS organiza jerárquicamente la asignación de rutas intradominio, permitiendo que un dominio grande sea divido en áreas pequeñas de fácil administración usando niveles. Nivel 1 para SI dentro de áreas y el Nivel 2 para SI entre áreas. El direccionamiento entre dominios administrativos es manejado por Border Intermediate Systems (BISs) usando Inter-Domain Routing Protocol. (IDRP).

Como cualquier protocolo de enrutamiento de Internet, IS-IS soporta grandes dominios de enrutamiento, los que incluyen muchos tipos de subredes individuales. Estas subredes pueden incluir enlaces punto a punto, enlaces multipunto, establece dinámicamente enlaces de datos como subredes en X.25 y subredes de transmisión usando ISO 8802 LANs. Dentro de IS-IS, todos los tipos de subredes son tratados como subredes independientes, como si no estuvieran enlazadas, usando funciones de convergencia si es necesario. Al igual que OSPF, IS-IS utiliza el algoritmo Shortest Path First SPF (primero el camino más corto) para determinar las rutas. Un componente de control de congestión supervisa y previene el punto muerto del buffer en cada sistema intermedio.

La sintaxis de configuración GateD permite tanto auto configuración como posibilita la reducción de probabilidades de error. Esta integración también permite la habilidad para especificar políticas de intercambio de información de enrutamiento con otros protocolos que corren GateD como BGP, EGP, RIP y IDRP. El nuevo protocolo IS-IS soporta Multi-dirección (Multipath) Load-Split ó división de carga en el envío de paquetes. Permite también una completa inyección de prefijos para redes exteriores, así como información de atributos con el objetivo de eliminar la necesidad de un Interior BGP o cualquier otro protocolo similar. Soporta también información de enrutamiento de dominios estáticos en el nivel 2 de los Sistemas Intermedios.

1.2.11. **Routing Information Protocol (RIP)**[17]

Routing Information Protocol ó más comúnmente conocido como RIP, es uno de los protocolos más antiguos en el enrutamiento de paquetes. Utiliza algoritmos de Vector-Distancia para calcular sus rutas, los cuales han sido utilizados por décadas en sus varias

[17] Routing Information Protocol (RIP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm. 2006-09-12.

versiones e inclusive este tipo de algoritmos fue utilizado por ARPANET en el año 1969. El protocolo RIP, tal cual se lo conoce actualmente, fue descrito por primera vez en el RFC 1058 en Junio de 1988 por C. Hedrick de la Rutgers University, y luego en Internet Standard STD 56. Consecuentemente el Internet Engineering Task Force (IETF) libera una nueva definición de RIP en el RFC 1388 en enero de 1993.

Para noviembre de 1994 se describe la nueva versión de RIP 2 en el RFC 1723 y posteriormente fue mejorado en la RFC 2453 por G.Malkin de la compañía Bay Networks en Noviembre de 1998. Desde el año 1998 el protocolo RIP se ha mantenido estable, pero posteriormente salió la versión RIP para Ipv6, la cual tiene su propio capítulo. RIPv2 incorpora nuevas características que valen la pena señalar como el soporte para máscaras de subredes, el uso de mecanismo de autenticación para la actualización segura de las tablas de ruteo.

RIP es un protocolo de enrutamiento de vector-distancia muy extendido en todo el Mundo, por su simplicidad en comparación a otros protocolos como OSPF, IS-IS o BGP. RIP es un protocolo abierto a diferencia de otros protocolos de enrutamiento como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies. RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada enrutador atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector-distancia no tiene en cuenta datos tales como por ejemplo, ancho de banda o congestión del enlace.

Actualizaciones de Ruteo.- RIP envía los mensajes de actualización de rutas a intervalos regulares y cuando la topología de la red a cambiado. Cuando un ruteador recibe una actualización que incluye un cambio en alguna ruta, este cambio es reflejado en la tabla de rutas. Los ruteadores RIP mantienen únicamente las mejores rutas hacia un destino, es decir la ruta con el menor costo. Después de actualizar la tabla de ruteo, el ruteador inmediatamente envía las actualizaciones de la topología sus demás vecinos dentro de la red. Estas actualizaciones son enviadas independientemente de las actualizaciones regulares.

Métricas de Enrutamiento RIP.- RIP utiliza una métrica simple de enrutamiento llamada Conteo de Saltos (Hop Count) para medir la distancia entre un origen y un destino dentro de una red. Cada salto en una ruta desde un origen hacia un destino es asignado a un valor de conteo de saltos con un típico 1. Cuando un ruteador recibe una actualización de ruteo que contiene un nuevo cambio a un destino dentro la red, el ruteador añade 1 a la métrica de valor indicada y lo ingresa en la tabla de rutas. La dirección IP enviada es utilizada como el siguiente salto.

Características de Estabilidad RIP.- Rip previene que los lazos de enrutamiento continúen indefinidamente por la implementación de un número de saltos para una dirección desde la fuente hacia el destino, siendo el número máximo de saltos para una dirección de 15. Si un ruteador recibe una actualización de información de enrutamiento que indica que una ruta hacia un destino tiene como métrica de salto 16, entonces se dice que este destino es considerado inalcanzable. Esta característica ha sido desarrollada con el fin de proveer estabilidad al protocolo.

Cronómetros RIP.- Rip utiliza numerosos cronómetros para regular su rendimiento. Incluye un cronómetro de actualización de enrutamiento, un cronómetro de interrupción de ruta y un cronómetro de vida de ruta. Estos contadores ayudan a prevenir la congestión dentro de una red.

1.3.VENTAJAS Y DESVENTAJAS.

1.3.1. **Ventajas.**

Entre los valores agregados de las redes de alta velocidad, se puede decir que representan una de las mayores participaciones en el mercado de las telecomunicaciones a nivel mundial. Esta importancia hace que dichas redes se consideren vitales para el desarrollo tecnológico de servicios informáticos, asociados tradicionalmente al procesamiento de datos, de tal forma que puedan ser aprovechados de manera vertical dentro de las empresas y de manera horizontal en las compañías con las que mantienen relaciones comerciales.

Dentro de las principales ventajas que las redes de alta velocidad prestan podemos citar las siguientes: grandes anchos de banda, elevada velocidad para video conferencias, soporte efectivo para enlaces multimedia, soporte para servicios en tiempo real, transmisión de grandes paquetes de información, soporte a muchas aplicaciones que involucran elevados anchos de banda como bases de datos distribuidas o bases de datos multidimencionales.

1.3.2. **Desventajas.**

Así como se presentan ventajas dentro de las redes de alta velocidad, también aparecen las desventajas, que en proporción son mucho menores, pero no por ello hay que hacerlas a un lado. Entre las desventajas más notorias de las redes de alta velocidad se puede señalar algunas como:

Elevados costos de equipamiento y mantenimiento para el usuario, por lo que no todas las empresas o entidades pueden disponer o está a su alcance este tipo de tecnología;

Necesidad de capacitación permanente por parte de los administradores, dado que día a día aparecen novedades que deben ser subsanadas con eficiencia y en el menor tiempo posible;

Costos de soporte técnico apropiado en el caso de que los problemas o inconvenientes se salgan de las manos del administrador local; y,

Necesidad de conocimientos especializados para la administración y operatividad de este tipo de redes y enlaces de alta velocidad.

1.4.APLICACIONES GENERALES.

Las aplicaciones para las redes de alta velocidad en la actualidad son prácticamente infinitas, dado el crecimiento que día a día tienen las empresas así como su necesidad de disponer de la información de forma permanente y al instante. Es valioso recordar que el verdadero tesoro que manejan las empresas hoy en día es la información, la cual debe ser manejada de forma segura, rápida y estar disponible en el momento que sea necesaria de forma eficiente.

Es así, que prácticamente las redes de alta velocidad han sido implementadas en casi todas las áreas donde se necesita que la información esté disponible al instante, como: hospitales, aeropuertos, centros de investigación, campus universitarios, complejos industriales, corporaciones transnacionales, industrias petroleras, agencias de inteligencia, laboratorios, NASA, etc.

Los grandes volúmenes de información transmitida a través de las redes tanto internas (Intranets), como externas (Internet), hacen que la importancia de las redes de alta velocidad sea cada día más elevada y por ende la investigación dentro de este capo, se vaya desarrollando cada día a un nivel en el cual muy pocos campos de investigación se pueden comparar.

CAPITULO II

TENDENCIAS, TECNOLOGÍAS Y ARQUITECTURAS EN REDES DE ALTA VELOCIDAD

2.1. Tendencias de redes de alta velocidad.

2.2. Tecnologías y arquitecturas más Importantes.

2.3. Clasificación de tecnologías y Arquitecturas.

2.4. Características principales.

2. TENDENCIAS, TECNOLOGÍAS Y ARQUITECTURAS EN REDES DE ALTA VELOCIDAD

2.1.TENDENCIAS DE REDES DE ALTA VELOCIDAD.

El desarrollo tecnológico que involucra todo el mundo de las redes y telecomunicación, continua uniendo esfuerzos con el único fin de ir aumentando el rendimiento de las redes. Una estrategia muy utilizada es aumentar la velocidad en las redes existentes a través de nuevas formas de compresión de datos o presentación de la información. Sin embargo, esta necesidad de reducir el tamaño de los archivos ó paquetes para aumentar la velocidad de entrega puede ser un asunto que tenga su tiempo de vida limitado, dado que los enlaces para la transmisión de información en banda ancha y las capacidades de transferencia de datos a altas velocidades en forma inalámbrica, se desarrollarán ampliamente durante los próximos 5 a 10 años para respaldar todo lo que involucra la investigación, comercio electrónico y el entretenimiento, que son los puntales del Internet de hoy en día.

Las tendencias de crecimiento, el cambio constante y las necesidades en diversas áreas obligan al desarrollo de nuevas tecnologías. Entre los puntos importantes de desarrollo tecnológico se encuentran las siguientes.

- Estaciones con mayor poder de cálculo.
- Poder y complejidad de aplicaciones.
  - Proceso distribuido de datos.
  - Información Multimedia.
  - Video conferencia.
  - Visualización / Realidad virtual.
  - Computer-Aided Designed (CAD).
  - Conectividad con usuarios móviles.
- Tamaño de archivos.
- Centralización de servidores.
- Aumento del ancho de banda de los enlaces.
- Incremento en el número de usuarios de red.
- El tráfico de datos normalmente es "asíncrono", con poca sensibilidad al retardo.
- Las nuevas aplicaciones con voz, multimedia, video son sensibles al retardo, hay que cuidar dónde es necesario garantizar el Acceso, Throughput (Caudal de proceso y transferencia) y Latencia.

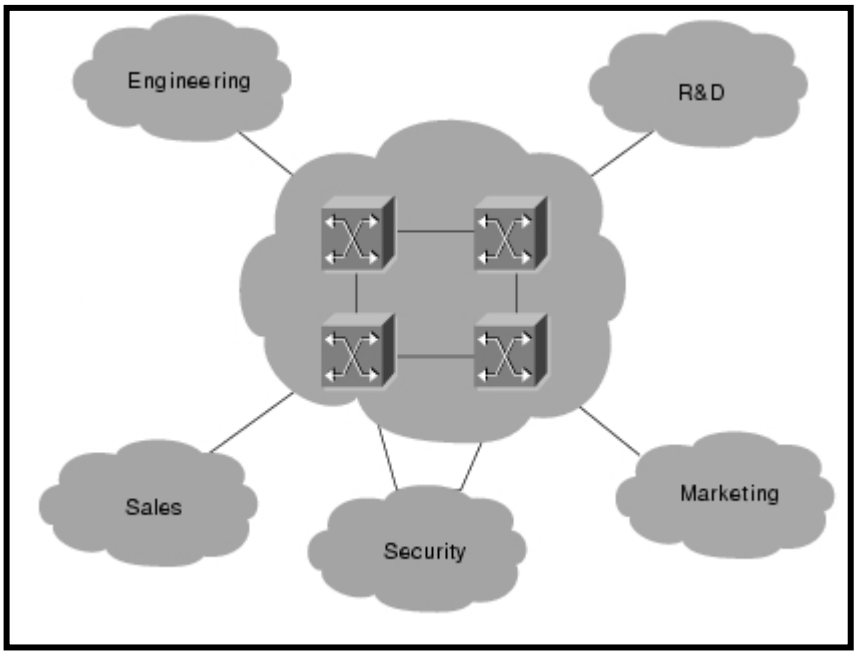


Fig: 2.1: Servicio dentro de una topología de red

FUENTE: Bridging Basics. Cisco Documentation: 2006-09-12
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bridging.htm.

La creciente utilización de servicios como cable módem y DSL para el uso residencial facilitará la comprensión de las inquietudes acerca del ancho de banda en el extremo del usuario. Una de las tendencias más importantes de las redes de alta velocidad es el potencial que proporciona a la televisión digital, en especial la Televisión de Alta Definición (HDTV), para proporcionar nuevos y diferentes tipos de información a una gran gama de usuarios; estos servicios pueden incluir el acceso a recursos culturales digitalizados por ejemplo.

Otro punto muy importante dentro de las tendencias de las redes de alta velocidad es la nueva versión de Internet, más comúnmente conocido como Internet2, en el cual el gobierno de los Estados Unidos está financiando esfuerzos para construir la Internet de la Próxima Generación (NGI), con el fin de unir los laboratorios de investigación y las universidades a redes de alta velocidad que son entre 100 a 1000 veces más rápidas que la Internet actual. Está diseñada para manejar grandes volúmenes de información, así que la NGI facilitará el acceso a las imágenes digitales, y volverá práctico el audio de alta calidad y la transferencia de imágenes en movimiento. Otras redes que se unen al Internet 2 son CA*net3 en Canadá; en Europa por GEANT (antes TEN 155) y en Asia por APAN, todas ellas compuestas por redes de alta velocidad. Con estos antecedentes todo apunta a que las redes de alta velocidad se tomen todo el mercado de las telecomunicaciones y prácticamente absorberán a las redes que funcionan actualmente.

2.2.TECNOLOGÍAS Y ARQUITECTURAS MÁS IMPORTANTES.

El estado actual de las telecomunicaciones y los servicios de datos en redes metropolitanas MAN y redes de área amplia WAN, se encuentran en una etapa de plena integración junto con las nuevas tecnologías que van apareciendo cada día. Las tecnologías en redes de alta velocidad para ambientes MAN y WAN, así como para las redes de transporte existentes hasta ahora, han experimentado un gran avance técnico y tecnológico, permitiendo brindar a los usuarios finales accesos a múltiples servicios de banda ancha con mejor calidad, rapidez y eficiencia, permitiendo así optimizar recursos.

El crecimiento de las redes, así como el despliegue de aplicaciones con un alto consumo de ancho de banda, hacen que el conocimiento de las arquitecturas y redes de alta velocidad sean esenciales. Por este motivo, analizaremos las arquitecturas de redes de alta velocidad y las diferentes soluciones, como Fast Ethernet y GigaEthernet, FDDI, ATM, X.25 y Frame Relay.

2.2.1. **SMDS**[18]

Switched Multi-megabit Data Service, o Servicio de Conmutación de Datos Multi-megabit es más que una tecnología, es un servicio completo de conmutación de paquetes de alta velocidad basado en la estructura de la tecnología de redes WAN, usado para la comunicación a través de redes de datos públicas. Permite la comunicación eficiente entre redes LAN y al mismo tiempo es un servicio público como las redes de área metropolitana MAN. Es capaz de proporcionar un transporte de datos transparente, "no orientado a conexión" entre abonados, utilizando accesos de alta velocidad de las redes públicas.

SMDS puede usar medios de comunicación de fibra o basados en cobre y soportar velocidades entre los 1.544 Mbps sobre Señales Digitales de Nivel 1 (DS-1), y los 44.736 Mbps sobre Señales Digitales de Nivel 3 (DS-3). Además, las unidades de datos de SMDS son lo suficientemente grandes para encapsular completamente IEEE 802.3, IEEE 802.5, y las tramas de Fiber Distributed Data Interface (FDDI).

[18] Switched Multimegabit Data Service (SMDS). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/smds.htm. 2006-09-12.

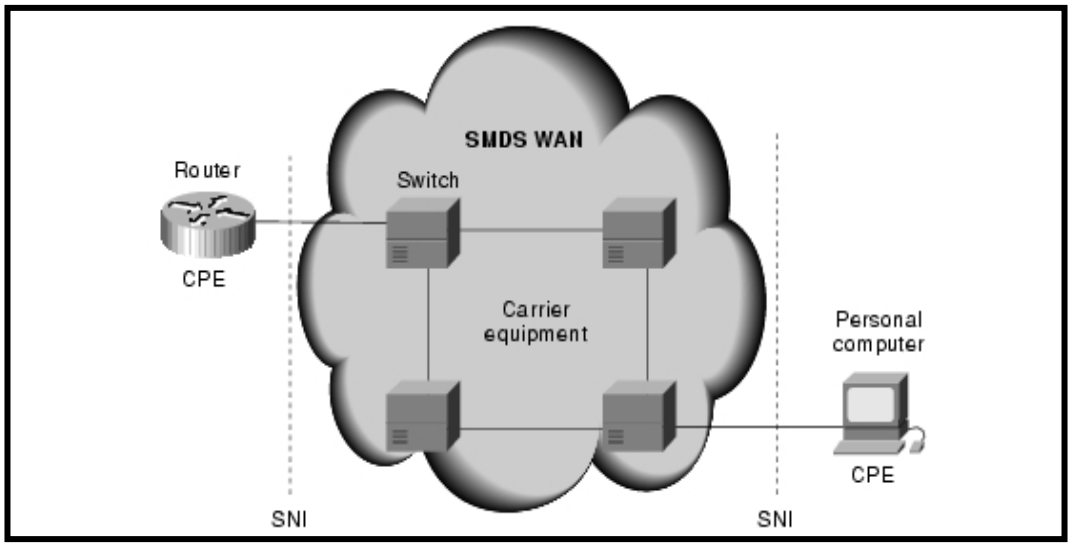


Fig: 2.2: Topología de un Red SMDS
FUENTE: Referencia [18].

SMDS se considera una red WAN pública, que extiende los servicios de las redes LAN y MAN, ya que su objetivo primordial es el de proporcionar conectividad para MAN's, subredes FDDI, y redes LAN privadas, de modo que compartir los datos sea tan fácil como realizar una llamada telefónica, y soportando tanto datos como voz y vídeo.

2.2.1.1. Componentes de una Red SMDS.

Las redes SMDS consisten en una serie de dispositivos conectados para proveer servicios de datos de alta velocidad. Los componentes principales son: Customer Premises Equipment (CPE) ó Equipamiento Local de Usuario, Equipos de Comunicación y Subscriber Network Interface (SNI) ó Interface de Suscriptor de Red. CPE incluye equipos finales tales como terminales y computadores personales, nodos intermedios como ruteadores, modems y multiplexores. Los equipos del proveedor generalmente consisten en los switches WAN de Alta Velocidad y algunas veces los equipos de los nodos intermedios de acuerdo a la estructura de la red.

El SIN es la interface entre el CPE y los equipos del proveedor. Esta interface es el punto donde finaliza de red de usuario y comienza la red del proveedor. La función del SIN es hacer que la tecnología y las operaciones del proveedor de red SMDS sean transparentes para el usuario final.

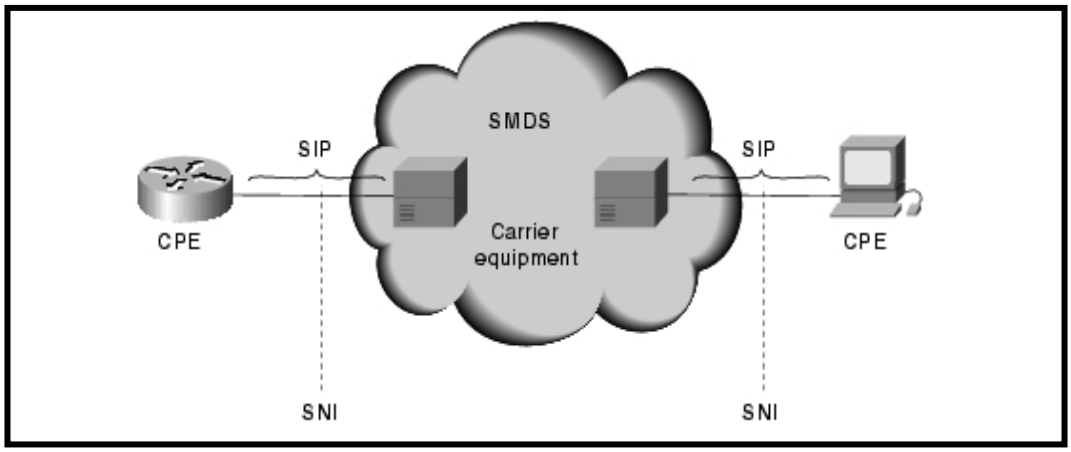


Fig: 2.3: Componentes de una Red SMDS
FUENTE: Referencia [18].

2.2.1.2. SMDS Interface Protocol (SIP).

El Protocolo de Interface SMDS, (SIP) por sus siglas en inglés es utilizado para las comunicaciones entre el CPE y el los equipos del proveedor de SMDS. SIP proporciona el servicio de conexión a través del Suscriber Network Interface (SNI), permitiendo al CPE acceder a la red SMDS. SIP está basado en el estándar Distributed Queue Dual Bus (DQDB) IEEE 802.6, para el transporte de celdas a través de redes de área metropolitana MAN. DQDB fue elegido como la base para SIP porque es un estándar abierto que soporta todas las características de servicio de SMDS; además DQDB fue diseñado para proveer compatibilidad entre los existentes equipos de transmisión. También se encuentra alineado con los estándares que emergieron para Broadband ISDN (BISDN), con lo que se permite la interoperatividad con los servicios de video y voz.

2.2.1.3. Distributed Queue Dual Bus (DQDB).

El DQDB es un protocolo de comunicación de la capa de enlace de datos, diseñado para el uso dentro de redes de área metropolitana (MANs), que especifica la topología de la red, compuesta de 2 buses lógicos unidireccionales para interconectar múltiples sistemas. Así está definido en el estándar IEEE 802.6 DQDB, donde un acceso DQDB, describe solo la operación del protocolo DQDB a través de la interface de usuario de red dentro de un SIN.

Un acceso DQDB se forma de los siguientes componentes de red SMDS:

- Carrier Equipment.- switch en la red SMDS que opera como estación;
- CPE.- que es uno o más dispositivos como estación de bus;
- SNI.- que actúa como interface de comunicación entre el CPE y el carrier equipment.

SMDS permite el manejo de Clases de Acceso para manejar un rango de broadcast de acuerdo al requerimiento de tráfico o capacidades de los equipos. Como es conocido que en todo tipo de redes, mientras más alta es la demanda de tráfico, el rendimiento de la red empieza a disminuir; es por este motivo que SMDS maneja este tipo de administración con el fin de mantener los servicios en el mejor estado posible.

2.2.2. **X.25**[19]

X.25 es un protocolo estándar de ITU-T (International Telecommunication Union-Telecommunication Standardization Sector), desarrollado para comunicaciones en redes WAN, que define como se establecen y mantienen las comunicaciones entre dispositivos usuario y dispositivos de red. Ha sido diseñado para operar de forma indiferente al tipo de sistemas conectados a la red y es típicamente usado en las redes de switcheo de paquetes (PSNs), tal como las compañías de teléfonos. El desarrollo del estándar X.25 fue iniciado por los proveedores de servicios en 1970, ya que en ese tiempo había la necesidad de protocolos WAN capaces de proveer conectividad a través de las redes públicas de datos (PDNs). Actualmente es administrado por la organización de estandarización internacional ITU-T.

Los equipos de red X.25 caen dentro de 3 categorías: Equipos Terminales de Datos (DTE), Equipos de Terminación de Circuitos de Datos (DCE) y los Equipos de Intercambio y Switcheo de Paquetes (PSE). Los Equipos Terminales de Datos son los dispositivos de sistema finales, que se comunican a través de una red X.25, y usualmente son terminales, computadores personales o host de una red y están localizados en grupo ó como suscriptores individuales. Los dispositivos DCE son equipos de comunicaciones; tales como modems y shitches de empaquetamiento y su función es proveer la interface entre los dispositivos DCE y PSE; y generalmente están localizados en los centros de servicio de los proveedores de servicios.

[19] X.25 Overview. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/x25.htm. 2006-09-13.

Los dispositivos PSE son switches que componen el núcleo central de la red del proveedor de servicios. Ellos se encargan de transportar los datos desde un dispositivo DTE hacia otro a través de PSE X.25. En la siguiente figura se muestra las relaciones entre estas tres categorías de dispositivos de X.25

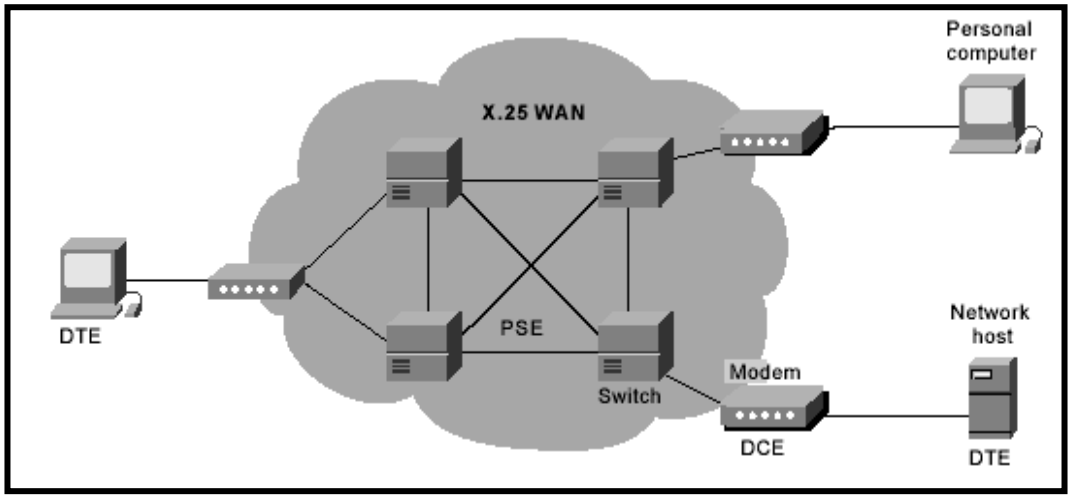


Fig: 2.4: Topología de una Red X.25

FUENTE: Referencia [19].

X.25 implementa circuitos virtuales para proporcionar comunicaciones seguras entre 2 dispositivos de una red. Además muchos circuitos virtuales pueden ser multiplexados a través de un simple circuito físico o enlace. Existen 2 tipos de circuitos virtuales: los circuitos switchados y los circuitos permanentes. Los Switched Virtual Circuits (SVCs) son conexiones temporales usadas esporádicamente para transferir datos, lo cual implica que dos dispositivos DTE establezcan, mantengan y terminen una sesión cada vez que necesiten comunicarse. Los Permanent Virtual Circuits (PVCs) son conexiones establecidas permanentemente usadas frecuentemente para transferir datos. Este tipo de circuitos no necesita que las sesiones de conexión sean terminadas. Este circuito permite transferir datos cuando sea necesario ya que la sesión siempre está activada.

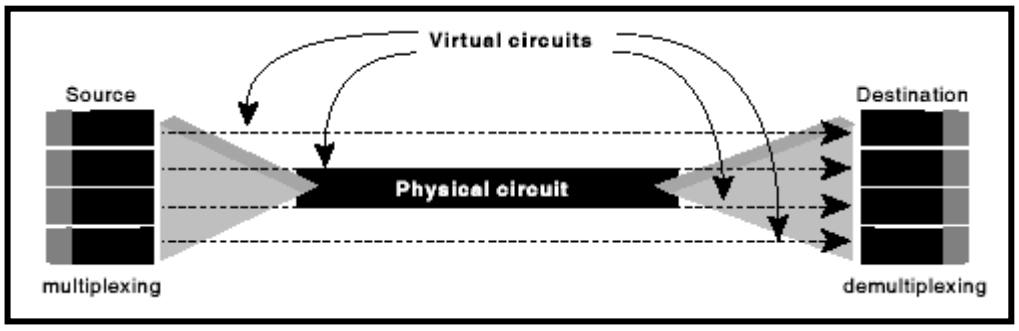


Fig: 2.5: Circuitos Físicos y Virtuales de X.25

FUENTE: Referencia [19].

El protocolo suite X.25 opera en las tres capas más bajas del modelo OSI, y dentro de este suite se encuentran los siguientes: Packet Layer Protocol (PLP), Link Access Procedure, Balanced (LAPB) y entre otros los protocolos de interface serial de capa física como X.21bis, EIA/TIA.232, EIA/TIA-449, EIA.530 y G.703.

2.2.3. **FRAME RELAY**[20]

Frame Relay es un protocolo WAN de alto rendimiento que opera en la capa física y de enlace del modelo OSI, siendo originalmente diseñado para ser usado entre interfaces ISDN Integrated Services Digital Network. Hoy en día es muy usado sobre una gran variedad de interfaces de red. Frame Relay es un ejemplo de tecnología de switcheo de paquetes y se utiliza principalmente para la interconexión de redes LAN y WAN sobre redes públicas o privadas.

Frame Relay nació del mismo grupo de normalización que dio lugar a X.25 y RDSI y se originó a partir de las interfaces ISND, siendo propuesto como estándar al Comité Consultivo Internacional para Telegrafía y Telefonía CCITT en 1984; pero el mayor desarrollo tecnológico en la historia de Frame Relay fue en el año de 1990 cuando Cisco, Digital Equipment Corporation DEC Northern Telecom. Y StrataCom formaron un consorcio enfocado en el desarrollo de Frame Relay. Este consorcio desarrolla las especificaciones que conforman la parte básica del protocolo Frame Relay el cual fue discutido en el CCITT, pero fue extendido a protocolo por las características adicionales que provee a ambientes de redes complejas.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para operar a velocidades de hasta 2,048 Mbps, aunque nada le impide superarlas. Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

[20] Frame Relay. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm. 2006-09-12.

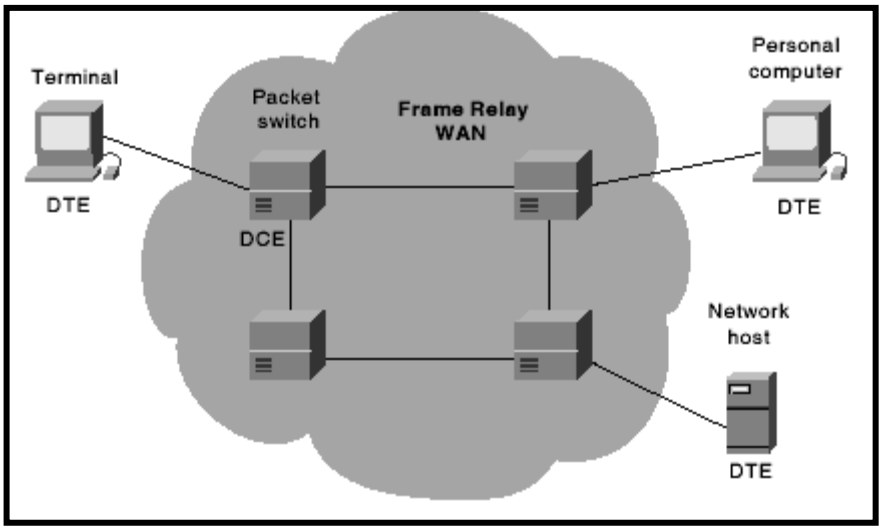


Fig: 2.6: Topología de una Red Frame Relay

FUENTE: Referencia [20].

Frame Relay al haber sido desarrollado mucho después que la tecnología X.25, se adapta mejor a las características de las infraestructuras de telecomunicaciones actuales. La norma está descrita sólo sobre las dos primeras capas o niveles del modelo OSI, a diferencia de X.25, que llega hasta el Nivel 3 de red, en el cual se consignan las funciones de control del flujo y la integridad de los datos. Por tanto, al no realizar estas funciones de control, Frame Relay resulta mucho más rápido que X.25, el cual fue concebido inicialmente para operar con circuitos analógicos utilizando procedimientos de control de errores, frecuentemente pesados, lentos y complejos.

En todos estos aspectos técnicos especificados anteriormente reside la fuerza de Frame Relay, además, permite al usuario pagar sólo por la velocidad media contratada y no sobre el tráfico cursado. El ancho de banda de trabajo normal de Frame Relay está entre los 64 Kbps y los 2.048, Mbps aplicándose también un concepto importante llamado "El ancho de banda bajo demanda" (Bandwidth on Demand), lo que permite la asignación del ancho de banda de forma dinámica. Al eliminar Frame Relay, muchas funciones superfluas de los niveles 2 y 3 del modelo OSI permite reducir el proceso de control en los nodos y el retardo, por ello Frame Relay admite la transmisión de voz.

En resumen, Frame Relay es un servicio rápido de conmutación de paquetes de longitudes variables, para transportar datos sobre áreas extensas. Es una evolución de X.25 que tiene la ventaja de una transmisión de mejor calidad, con mayor rapidez y reduciendo el encabezado de chequeo de errores. Frame Relay soporta velocidades de transmisión de hasta 2 Mbps. Está controlado por los estándares ANSI T1.617 anexo D y el UIT-T Q.933 anexo A.

2.2.3.1. Dispositivo Frame Relay.

Los dispositivos asociados a redes WAN Frame Relay caen dentro de 2 grandes categorías; La primera es Data Terminal Equipment (DTE) y la otra es Data Circuit-Terminating Equipment (DCE). Los dispositivos DTEs generalmente son considerados como equipos de finalización para redes específicas y típicamente están en posesión de los usuarios finales y pueden ser terminales, computadores personales, ruteadores o bridges. Los dispositivos DCEs son los equipos de comunicación de la red Frame Relay y el propósito de estos equipos es proveer el reloj y los servicios de switcheo dentro de la red, permitiendo la actualización de la trasmisión de datos a través de la WAN. En muchos de los casos son equipos de empaquetamiento.

2.2.3.2. Circuitos Virtuales Frame Relay.[21]

Frame Relay provee una conexión de datos orientada a enlace. Esto significa que la comunicación existente entre cada par de dispositivos y esta conexión, está asociada con un identificador de conexión. El servicio es implementado utilizando Circuitos virtuales Frame Relay, con la creación lógica de una conexión entre dos dispositivos Data terminal Equipment (DTE), a través de una red de switcheo de paquetes Frame Relay. Los Circuitos Virtuales Frame Relay permiten una ruta de comunicación bidireccional, desde un dispositivo DTE hacia otro utilizando un identificador de conexión para el enlace de datos creado.

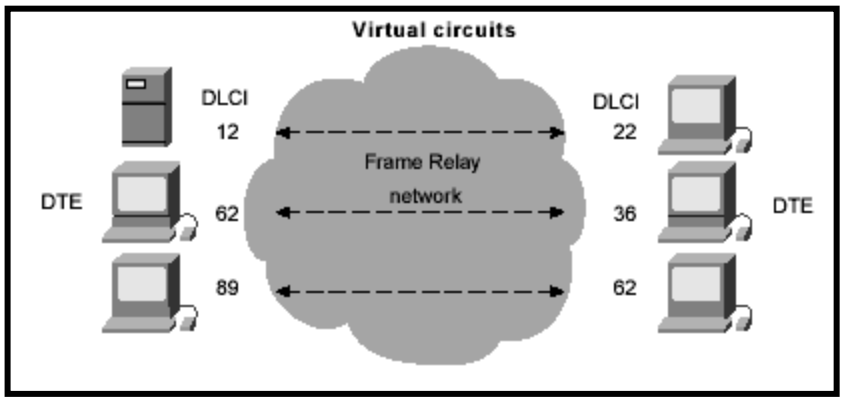


Fig: 2.7: Circuitos Virtuales en Frame Relay

FUENTE: Frame Relay. Cisco Documentation: 2006-09-12
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm.

[21] Interconecting Cisco Network Devices, Vol.1 version 2.3 Student Guide ICND 2.3. Año 2006.

El número de circuitos virtuales puede ser multiplexado dentro de un simple circuito físico para la transmisión a través de una red. Esta capacidad a menudo puede reducir el equipamiento y complejidad requerida para conectar múltiples dispositivos DTE. Un circuito virtual puede pasar por cualquier número de dispositivo DCE intermedios (switches) localizados dentro de una red de switcheo de paquetes. Los circuitos virtuales Frame Relay se clasifican en dos categorías: Circuitos Virtuales Switchados (SVCs) y en Circuitos Virtuales Permanentes (PCVs).

- ***Circuito Virtuales Switchados (SVCs)***.- Son conexiones temporalmente usadas en situaciones requeridas solo para transferencia de datos esporádicos entre dispositivos DTE a través de una red Frame Relay. Luego de terminada la transferencia de datos y es cerrado el circuito virtual, se hace necesario crear un nuevo circuito si se desea volver a transferir datos entre los mismo dispositivos DTE.

- ***Circuitos Virtuales Permanentes (PCVs)***.- Son conexiones establecidas permanentemente ya que son usadas para frecuentes y consistentes transmisiones de datos entre dispositivos DTE a través de una red Frame Relay. Las comunicaciones a través de PVC no requieren que la conexión sea iniciada y terminada como en los SVCs. Los PVCs siempre están operativos esperando o transmitiendo datos.

2.2.4. **ATM.**[22]

ATM (Asynchronous Transfer Mode) ó en español, Modo de Transferencia Asíncrono es un estándar de la International Telecommunication Union – Telecommunications Standars Section (ITU-T), cuyos primero estudios estuvieron disponibles en el año de 1988. ATM es una tecnología basada en la conmutación rápida de paquetes de tamaño pequeño y fijo de 53 bytes a los cuales se les denomina Celdas ATM. Las redes ATM están orientadas a conexión por lo que antes de iniciarse el intercambio de datos se debe establecer un proceso de asignación de recursos y de identificación interna del flujo de datos.

Este proceso da como resultado la creación de los circuitos virtuales mediante los cuales se realizan las comunicaciones, es así que se puede permitir mantener múltiples comunicaciones con uno o varios destinos a la vez. El desarrollo de esta tecnología nació

[22] Asynchronous Transfer Mode (ATM) Switching. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm. 2006-09-12.

con el fin de poder proveer una red que soporte los múltiples tipos de servicios dentro de la información como video, voz y datos y los convierta en celdas pequeñas con un tamaño manejable para permitir un óptimo desempeño de los equipos y por consiguiente proveer un servicio eficiente de envió de información.

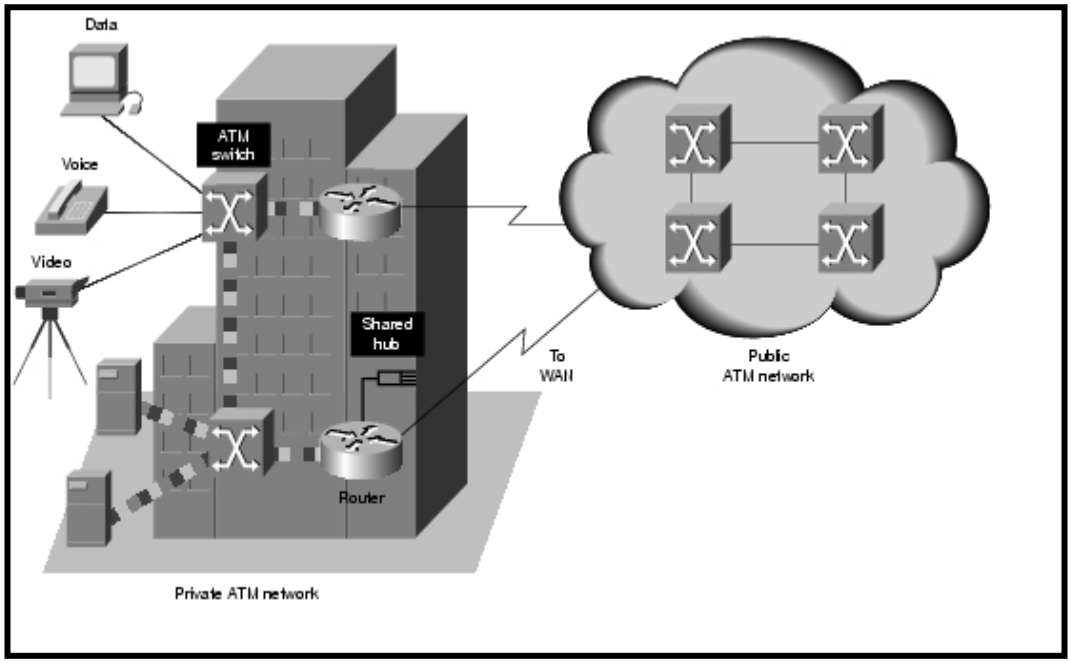


Fig: 2.8: Topología de una Red ATM
FUENTE: Referencia [22].

ATM es una tecnología que pretende resolver dos problemas muy importantes dentro de las tecnologías de red; uno es Mayor Ancho de Banda y el otro, Rápida Conmutación de Paquetes, lo que permitiría llevar los paquetes o tramas de un lado de la red hacia otro en el menor tiempo posible sin retrasos, ni pérdidas. Así, ATM se ha convertido en un servicio de transporte de celdas ATM extremo a extremo, donde las celdas ATM generadas por un equipo cliente son transportadas a un destino remoto de forma eficiente y fiable, con el mínimo retardo. ATM proporciona una multiplexación estadística de diferentes comunicaciones establecidas en circuitos virtuales de carácter permanente, permitiendo el compartir una misma línea de transmisión.

2.2.4.1. Aplicaciones de ATM.

Entre las aplicaciones típicas de ATM se encuentran, el Intercambio de información en tiempo real, dentro del ámbito empresarial; Interconexión de Redes de Área Local (LAN) que requieran un gran ancho de banda; Interconexión de PABX; Acceso a Internet

de alta velocidad; Videoconferencia; Voz en entorno corporativo con compresión y supresión de silencios; Distribución de Audio/Vídeo.

ATM se considera la única tecnología capaz de integrar todos los servicios disponibles hoy en día con los requisitos esperados de ancho de banda. Esto convierte a ATM en la mejor solución ante la necesidad de un medio de transporte único con capacidad multiservicio.

2.2.4.2. Ambiente de la Red ATM.

ATM es una tecnología de multiplexación y switcheo de celdas que combina los beneficios del switcheo, garantizando la capacidad y la constante transmisión de los paquetes switchados, así como flexibilidad y eficiencia para el tráfico intermitente. Esta característica proporciona un ancho de banda escalable desde unos pocos megabits por segundo (Mbps) hasta muchos megabits por segundo (Gbps). Así trabaja el modo asíncrono de ATM lo que incorpora más eficiencia que la tecnología síncrona como TDM Time-Division Multiplexing.

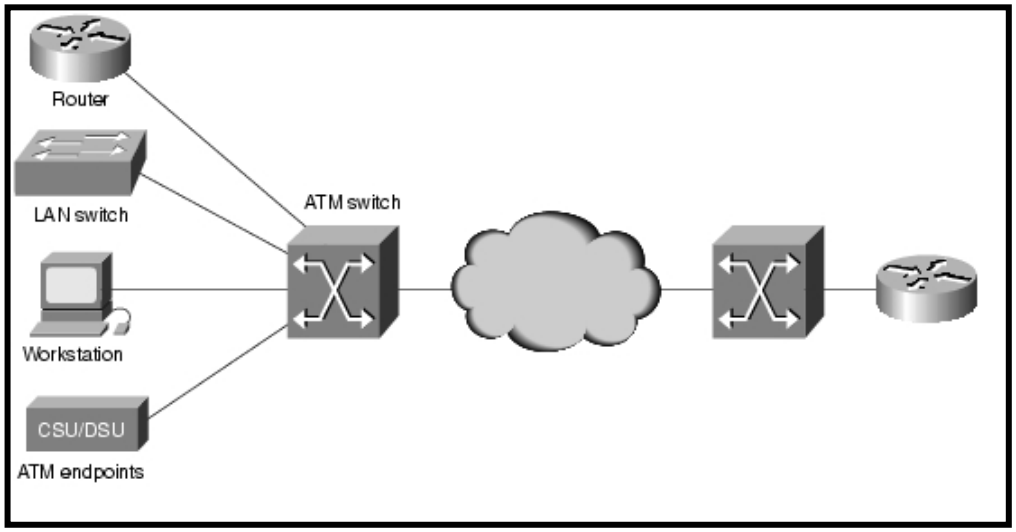


Fig: 2.9: Ambiente de una Red ATM

FUENTE: Referencia [22].

La multiplexación de ATM ofrece una ventaja adicional, y es la posibilidad de que trabaje tanto en modo de circuitos como en modo de paquetes. El modo de circuitos (por ejemplo, voz), se denomina también CBR o "Continuous Bit Rate"; el modo de paquetes, casi siempre datos, es denominado VBR ("Variable Bit Rate"). De este modo, se logra

compatibilidad con el equipamiento de red existentes, así como con todos los servicios de red. Las conexiones ATM, denominadas circuitos virtuales, pueden ser permanentes (PVC o Permanent Virtual Circuit), que operan como una línea física dedicada, creando una conexión permanente entre dos puntos de la red; o pueden ser conmutados (SVC o Switched Virtual Circuit), equivalentes a los de la red telefónica, donde las conexiones entre dos puntos de la red se establecen dinámicamente para cada transmisión.

Las celdas ATM son encaminadas entre dos puntos de la red a través de canales virtuales (VC o Virtual Channel) y caminos virtuales (VP o Virtual Path). Un canal virtual es la conexión entre dos entidades finales ATM, y ello conlleva el establecimiento de todos los enlaces necesarios para crear la comunicación entre dichas entidades. Los caminos virtuales son grupos de canales virtuales que conectan dos puntos finales, incluyendo todos los enlaces asociados a través de la red ATM. Son un medio muy conveniente para agrupar el tráfico de todos los canales virtuales con idéntico destino.

2.2.4.3. La Capa Física de la Red ATM.

La capa física de ATM tiene cuatro funciones: La primera función es convertir las celdas en bitstream; la segunda función es de transmisión y recepción de bits dentro del medio físico controlado; la tercera función es ATM cell boundaries are tracked y la cuarta función es el empaquetamiento de las celdas ATM dentro de los apropiados tipos de frames de acuerdo al medio físico.

ATM soporta dos tipos de conexiones que son: Punto a Punto y Punto a Multipunto. Las conexiones Punto a Punto enlazan dos sistemas ATM finales y pueden ser unidireccionales (un solo camino de comunicación) o bidireccionales (dos caminos de comunicación). Las conexiones Punto a Multipunto enlazan un origen simple ó nodo de ruteo con múltiples sistemas de destino finales conocidos como leaves. Estas conexiones son solamente unidireccionales. Los nodos de ruteo pueden trasmitir hacia los leaves pero los leaves no pueden trasmitir hacia los nodos de ruteo o hacia otro lugar en la misma conexión. Desafortunadamente las conexiones Multipunto a Multipunto todavía no han sido implementadas dentro del soporte tecnológico de las redes ATM.

2.3.CLASIFICACIÓN DE TECNOLOGÍAS Y ARQUITECTURAS.

En esta sección se realiza una breve clasificación y detalle de las tecnologías más importantes en redes de alta velocidad así como de la arquitectura que las rodea.

2.3.1. **Redes Digitales de Servicios Integrados.**[23]

Las Redes Digitales de Servicios Integrados (ISDN) están comprendidas por la telefonía digital y el transporte de datos y demás servicios ofrecidos por los proveedores de telefonía regional. ISDN involucra la digitalización de la red telefónica para permitir el transporte de voz, datos, texto, gráficos, video y otro tipo de material en una transmisión sobre las redes existentes de telefonía. ISDN representa un gran esfuerzo para suscribir la estandarización de servicios, interfaces de usuarios de red, las capacidades de una red e inter-red; así como las aplicaciones de ISDN que incluyen el manejo de aplicaciones de imagen de alta velocidad como los faxes, adicionalmente las líneas telefónicas de las casas permitirán las transferencia de archivos de alta velocidad y videoconferencia donde también están involucrados los servicios de voz.

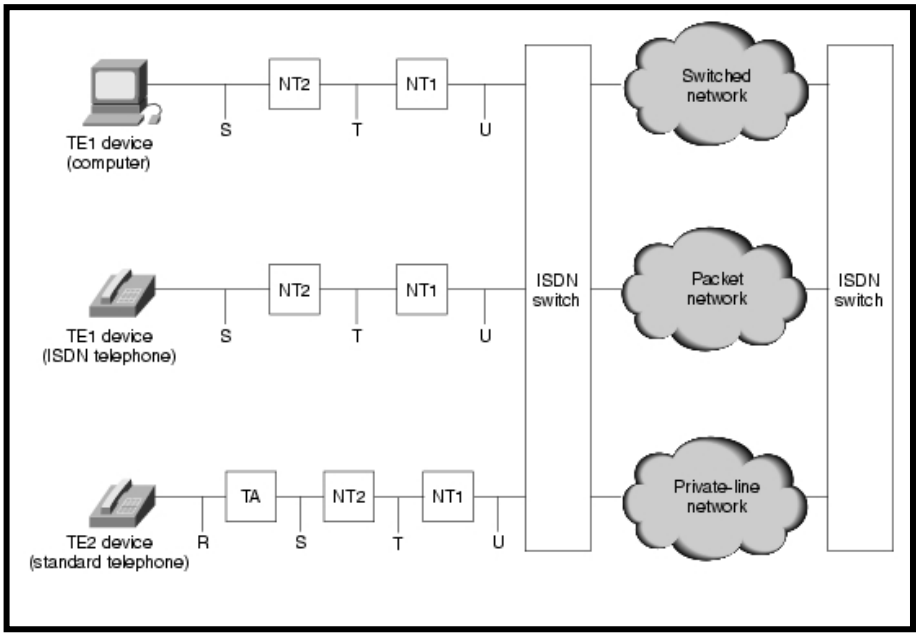


Fig: 2.10: Topología de una Red ISDN

FUENTE: Integrated Services Digital Network (ISDN). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/isdn.htm. 2006-09-13

La tecnología RDSI actual, también conocida como RDSI de banda estrecha, está basada en una de las dos estructuras definidas por Consultative Committee for International Telegraph and Telephone (CCITT).

- ***Acceso básico (BRI) que permite:***

[23] RDSI: Telefonía y Servicios Digitales: http://www.consulintel.es/Html/Tutoriales/Articulos/rdsi.html. 2001-11-10.

- Acceso simultáneo a 2 canales de 64 Kbps, denominados canales B, utilizados para voz o datos.
- Un canal de 16 Kbps., o canal D, para la realización de la llamada y otros tipos de señalización entre dispositivos de la red.
- En conjunto, se denomina 2B+D, o I.420, que es la recomendación CCITT que define el acceso básico. El conjunto proporciona 144 Kbps.

❖ ***Acceso primario (PRI) que permite:***

- Acceso simultáneo a 30 canales tipo B, de 64 Kbps., para voz y datos.
- Un canal de 64 Kbps., o canal D, para la realización de la llamada y la señalización entre dispositivos de la red.

Por evidencia notable, las comunicaciones vía RDSI, han de convivir con las actuales líneas de telefonía, por lo que es perfectamente posible establecer una llamada, por ejemplo; entre un teléfono RDSI y un teléfono analógico o viceversa, del mismo modo que es posible comunicar, vía RDSI, con X.25 o redes tipo Frame Relay, dada la versatilidad de este tipo de tecnologías.

2.3.2. **Frame Relay.**

Frame Relay constituye un estándar de comunicación orientado a switcheo de paquetes para permitir la conexión de sistemas de redes informáticos. Se utiliza principalmente para la interconexión de redes de área local (LANs, local área networks) y redes de área extensa (WANs, wide área networks) sobre redes públicas o privadas. La mayoría de compañías públicas de telecomunicación ofrecen los servicios Frame Relay como una forma de establecer conexiones virtuales de área extensa que ofrezcan unas prestaciones relativamente altas.[24]

Frame Relay es una interfaz de usuario dentro de una red de conmutación de paquetes de área extensa, que típicamente ofrece un ancho de banda comprendida en el rango de 56 Kbps y 1.544 Mbps. Así, Frame Relay se originó a partir de las interfaces ISDN y se propuso como estándar al Comité Consultivo Internacional para Telegrafía y Telefonía (CCITT) en 1984. El comité de normalización T1S1 de los Estados Unidos, acreditado por el Instituto Americano de Normalización (ANSI), realizó parte del trabajo y estudio preliminar sobre Frame Relay.

[24] Frame Relay: 1er estándar internacional que funciona: http://www.consulintel.es/Html/Tutoriales/Articulos/frame_relay.html. 2001-11-10.

Como parte importante de la estructura que opera Frame Relay se encuentra el manejo de Circuitos de Switcheo Virtual y los Circuitos Virtuales Permanentes. Además maneja mecanismos de control de congestión diseñados para permitir un correcto fluido de los paquetes dentro del enlace. Entre estos métodos de control de congestión se tiene la Elección de Descarte de tramas o paquetes de baja importancia y el Chequeo de Error de tramas usado cuando hay redundancia de paquetes en una transmisión.

2.3.3. **Gigabit Ethernet / Fast Ethernet.**[25]

La red Ethernet original se desarrolló como una red de cable coaxial experimental en 1970 por la Corporación Xerox, que operaba con un rango de datos de 3 Mbps usando el protocolo CSMA/CD para redes LAN con requisitos de tráfico esporádico pero ocasionalmente pesado. El éxito con ese proyecto llamó la atención y llevó en 1980 al desarrollo conjunto de 10-Mbps Versión de Ethernet 1.0 especificado por el consorcio de tres compañías: Digital Equipment Corporation, Intel Corporation y Xerox Corporation

El original IEEE estaba basado en la norma 802.3 y era muy similar a la especificación de Ethernet Versión 1.0. La norma del proyecto fue aprobada 3 en 1983 por el grupo de trabajo de 802.3 y luego fue publicada como estándar oficial en 1985 (ANSI/IEEE Std. 802.3-1985). Desde entonces, se han definido varios suplementos a la norma aprovechando las mejoras en la tecnología y apoyando los medios de comunicación adicionales y las capacidades más altas de transmisión de datos, así como las nuevas características de control de acceso a una red.

2.3.3.1. Fast Ethernet.

Para incrementar el radio de transmisión de Ethernet por un factor de diez sobre 10Base-T no era una tarea simple, y este esfuerzo terminó en el desarrollo separado de tres estándares de capa física para 100 Mbps sobre cable UTP: 100Base-TX y 100Base-T4 en 1995, y 100Base-T2 en 1997. Cada uno fue definido con diferentes requerimientos de codificación y diferentes juegos de configuración de los medios de transmisión. Aunque no todas las versiones de 100-Mbps tuvieron éxito en el mercado, todas tres se han discutido en la literatura y tuvieron su impacto en los diseños futuros.

[25] Gigabit Ethernet. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm. 2006-09-12.

100Base-X fue diseñado para soportar transmisión half-dúplex y full-dúplex sobre dos pares de alambres de cobre de cable UTP Categoría 5 ó dos hilos de fibra óptica. Aunque la codificación, decodificación y procedimientos de recuperación de reloj son los mismos para ambos medios, la señal de transmisión es diferente entre los pulsos eléctricos en cobre y los pulsos de luz en fibra óptica.

100Base-T4 fue desarrollado para permitir a las redes 10Base-T actualizarse a operar a 100 Mbps sin el requerimiento de existir 4 pares de alambres, por lo que no era necesario reemplazar el cable UTP Categoría 3 por el nuevo UTP Categoría 5. Dos de los pares son configurados para operación half-dúplex y pueden soportar transmisión en ambas direcciones, pero en una dirección a la vez. Los otros 2 pares son configurados como simples, dedicados para la transmisión en una sola dirección. La operación de transmisión full-dúlex no es soportada por 100Base-T4.

100Base-T2 fue desarrollada como una mejor alternativa para actualizar las redes instaladas con cable UTP Categoría 3 que la que proveía 100Base-T4. Dos nuevas importantes metas han sido definidas: a) Soportar comunicación sobre dos pares de cable Categoría 3 o un cable mejor, y b) Soportar ambos tipos de operación, half-dúplex y full-dúplex.

100Base-T2 utiliza un procedimiento diferente de señal de transmisión que las versiones anteriores de par trenzado Ethernet. En lugar de usar dos simples enlaces para formar un enlace full-dúplex, 100Base-T2 dual-dúplex de transmisión de banda base utiliza el método de envío de símbolos codificados simultáneamente en ambas direcciones sobre ambos pares de cables.

2.3.3.2. Gigabit Ethernet.

En marzo de 1996, el comité 802 de IEEE aprobó el proyecto estándar Gigabit Ethernet 802.3z; el mismo que fue desarrollado resultando en dos especificaciones primarias: 1000Base-T para cable de cobre UTP y 1000Base-X para cable de cobre STP así como cable de fibra óptica mono-modo y multi-modo. Además sigue manteniendo el método de acceso CSMA/CD para controlar el flujo de transmisión de datos en el medio de transmisión.

La capa física de Gigabit Ethernet, está formada por un mixto o híbrido entre la tecnología Ethernet y la Especificación de Canales por Fibra ANSI X3T11. Gigabit Ethernet es acepta finalmente 4 tipos de medios físicos, los cuales son definidos en 802.3z (1000Base-X) y 802.3ab (1000Base-T)

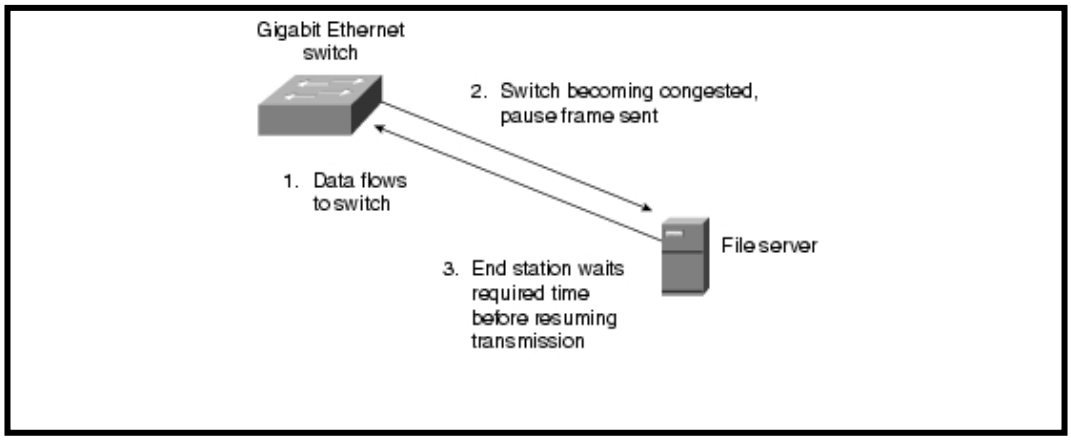


Fig: 2.11: Tecnología Gigabit Ethernet
FUENTE: Referencia [25].

1000Base-X en todas sus tres versiones soporta transmisión binaria full-dúplex a 1250 Mbps sobre dos hilos de fibra óptica o dos pares trenzados de cable de cobre STP. La transmisión se codifica basándose en el esquema de ANSI Fiber Channel 8B/10B. Todas las versiones de 1000Base-X en capa física soportan operaciones half-dúplex y full-dúplex. La principal diferencia entre las versiones 1000BaseX es el medio de enlace y los conectores que las particulares versiones soportan y, en el caso de medios ópticos, la longitud de onda de las señales ópticas.

En el estándar 1000Base-X la capa física es el Canal de Fibra. El Canal de Fibra es una tecnología de interconexión entre workstation, supercomputadoras, dispositivos de almacenamiento de información y periféricos. El Canal de Fibra tiene una arquitectura de 4 capas. La más baja tiene 2 capas FC-0 (Interfaz y Medio) y FC-1 (Codificador y Decodificador), estas son usadas en Gigabit Ethernet.

Hay 3 tipos de medios de trasmisión incluidos en el estándar 1000Base-X:

a) 1000Base-SX: usa una fibra multi-modo, 850nm.
b) 1000Base-LX: puede ser usada tanto mono-modo y multi-modo, 1300mn.
c) 1000Base-CX: usa un cable par trenado de cobre (STP).

1000Base-T ethernet proporciona transmisión full-duplex sobre 4 pares de cable UTP Categoría 5 o superior, ya que está basado enteramente en las búsquedas y diseños aprobados a lo largo del desarrollo de las implementaciones de Fast Ethernet en la capa física, así: 100Base-TX probó que cadenas de símbolos binarios pueden ser trasmitidas con éxito sobre cable UTP Categoría 5 a 125 MBd; 100Base-T4 proporcionó una básica comprensión de los problemas relacionados con el envío de múltiples señales sobre cuatro pares trenzados; y, 100Base.T2 probó la codificación PAM5.

2.3.4. **Servicios primarios de las redes ATM.**[26]

Con el objetivo de brindar mejor calidad en la transmisión de datos de cualquier tipo se diseña ATM, la cual puede ofrece calidad de servicio en el ancho de banda deseados en función de las necesidades de cada servicio, utilizando siempre el mismo soporte o medio físico de transporte. ATM es una técnica orientada a conexión entre 2 entidades, entre las que se establecerá un canal o camino de comunicación que se mantendrá durante todo el intercambio de información.

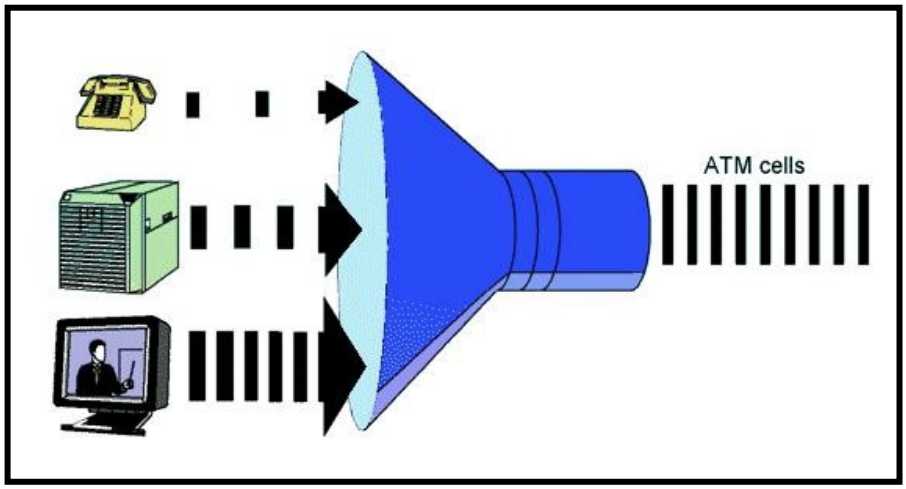


Fig: 2.12: Empaquetamiento de Celdas ATM

FUENTE: ATM (Asynchronous Transfer Mode): 2006-07-8.
http://html.rincondelvago.com/atm-asynchronous-transfer-mode_1.html.

La idea es dividir la información a transmitirse en paquetes de tamaño fijo, a los cuales se denominará células y que tienen un tamaño de 53 octetos, 48 de datos y 5 de cabecera. El canal de comunicación tendrá que ser compartido entre distintas conexiones para lo cual se divide en intervalos de tiempos iguales y en cada intervalo de tiempo se transmitirá una célula. El resultado será un flujo continuo de transmisión de células formado por flujos de menor capacidad. El ancho de banda usado por cada uno de estos flujos depende de las necesidades de la conexión a la que pertenecen.

De esta forma se consigue una multiplexión estadística y no estática, lo que optimiza el ancho de banda disponible, como se aprecia en la figura, la información de una misma conexión no aparece de forma periódica como ocurre en una multiplexión estática; de ahí el nombre de modo de transferencia asíncrono.

---

[26] ATM. Tutorial y descripción técnica TCP/IP:
http://ditec.um.es/laso/docs/tut-tcpip/3376c213.html#atm. 2000-07-14.

Resumiendo podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos dentro de este tipo de redes son capaces de encaminar la información empaquetada en células, a través de unos caminos conocidos como Conexiones de Canal Virtual. El routing, en los nodos conmutadores de células, es un proceso propio de hardware, mientras que el establecimiento de conexiones, el empaquetamiento y desempaquetamiento de las células son procesos puramente de software.

2.4.CARACTERÍSTICAS PRINCIPALES

Dentro de las características de cada una de las tecnologías de redes de alta velocidad detallaremos las más importantes y sobresalientes, así tenemos a continuación las siguientes:

2.4.1. **SMDS.**

Características:

- El interfaz de red a los locales del abonado se denomina Interfaz de Subred de abonado (SNI, Subscriber Network Interface). Las tramas "no orientadas a conexión" son enviadas sobre el SNI entre equipos de abonado y el equipamiento de la red pública.

- El formato de los datos y el nivel de adaptación es idéntico al especificado por IEEE 802.6. El SNI se especifica como un interfaz DQDB punto-a-punto, aunque el interfaz DQDB punto-a-multipunto no está excluido. El caso de bucle de bus dual no se ha contemplado por su complejidad y coste, y porque existen alternativas más simples para ofrecer esta redundancia.

- El nivel físico del SNI es el especificado por el estándar IEEE 802.6.

- Las direcciones fuente y destino conforman el estándar E164, junto con la posibilidad de broadcast y multicast de direcciones E.164.

- Capacidad de definir Grupos Cerrados de Usuarios mediante validación de direcciones tanto en salida como en destino.

2.4.2. **FRAME RELAY**

- Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto.

- Servicio orientado a conexión y puede ser de 2 tipos:

  - Circuito Virtual Permanente (PVC), donde cada conexión virtual entre dos abonados es establecido por el operador de la red en el momento de la subscripción y solo puede ser modificado por este.

  - Circuito Virtual Conmutado (SVC), en este caso debe existir un procedimiento de nivel 3 a fin de que los usuarios puedan establecer y liberar las conexiones a voluntad.

- Tecnología más liviana que no utiliza procedimientos de control de errores, frecuentemente pesados, lentos y complejos como X.25, pues Frame Relay trabaja solo en las 2 primeras capas del modelo OSI.

- Los nodos de extremo a extremo son los encargados del procesamiento y empaquetamiento de tramas.

2.4.3. **FAST ETHERNET (100 BASE-T).**

Características:

- Más de 2/3 de las redes actuales son ethernet.
- Plataforma dominante: 10 Base-T.
- En 100 Base-T(IEEE 802.3) se mantiene CSMA/CD.
- Topología de estrella.
- Nuevos esquemas de señalización.

Beneficios:

- 10 veces la velocidad de 10 Base-T a máximo el doble de costo.
- Tecnología probada.
- Sencillez de uso y migración, p.e. productos duales 10/100.
- Uso de plataformas de administrables existentes.
- Equipos de bajo costo.

2.4.4. **GIGABIT ETHERNET.**

Características:

- Creado por la alianza Gigabit-Ethernet(11 compañías) en 1996.
- Draft standard IEEE 802.3z en julio de 1997.
- Compatible con ethernet existente: CSMA/CD, full and half duplex.
- Slot time -> 512 bytes (8 veces más).
- 1000 Base-X basado en la capa física de Fibre Channel(FC0 and FC1), sobre fibra(3000m) o STP(25m).

2.4.5. **ATM.**

Características principales

- Los nodos de este sistema son equivalentes a una subred DQDB, y se interconectan por medio de una función de encaminamiento a nivel MAC con capacidad de re-encaminamiento automático.

- Un conjunto de servicios de transporte:
  Orientado a Conexión
  Orientado a No Conexión
  Isócrono
  Un doble bus de fibra como medio de transporte.
  Un Control de Acceso al Medio (MAC) que permite a los nodos compartir un medio de transmisión de forma más ecuánime.
  Capacidad de reconfiguración cuando se producen fallos.

- Las aplicaciones típicas de ATM son:
  Intercambio de información en tiempo real, dentro del ámbito empresarial.
  Interconexión de Redes de Área Local (LAN) que requieran un gran ancho de banda.
  Interconexión de PABX.
  Acceso a Internet de alta velocidad.
  Videoconferencia.
  Voz en entorno corporativo con compresión y supresión de silencios.
  Distribución de Audio/Vídeo.

CAPITULO III

ESTRUCTURA ORGANIZACIONAL DE PETROINDUSTRIAL

3.1. Estructura y enfoque de Petroindustrial filial de Petroecuador.

3.2. La Unidad de Sistemas dentro de la filial

3.3. Estructura y función de la Unidad de Sistemas

3. ESTRUCTURA ORGANIZACIONAL DE PETROINDUSTRIAL

En este capítulo vamos a referirnos a la estructura organizacional, misión y visión de Petroindustrial, así como a su importancia y enfoque empresarial. También describirá la estructura y función de la Unidad de Sistemas dentro del contexto operacional de la empresa.

3.1. ESTRUCTURA Y ENFOQUE DE PETROINDUSTRIAL, FILIAL DE PETROECUADOR.

3.1.1. **Misión.**

La Misión de Petroindustrial se ha definido como[27]:

"Producir combustibles y otros derivados del petróleo con estándares de calidad mundial, preservando estrictamente el medio ambiente y contribuyendo al desarrollo productivo del Ecuador."

3.1.2. **Visión.**

La Visión de Petroindustrial se ha definido como:

"Empresa de industrialización de petróleo, de propiedad del Estado Ecuatoriano, con capacidad estratégica, flexibilidad organizacional y cultura empresarial competitiva a nivel mundial, que opera con estándares internacionales de eficiencia y mantiene armonía con los recursos socio-ambientales."

3.1.3. **Objetivos de Petroindustrial.**

- ✓ Industrialización de los hidrocarburos, con la mayor eficiencia empresarial, previniendo la contaminación ambiental.
- ✓ Abastecer la demanda de los combustibles del país.

[27] SITE OFICIAL PETROINDUSTRIAL: http://www.petroindustrial.com.ec/frontEnd/main.php?idSeccion=7. Año 2005.

- ✓ Invertir en estudios de impacto ambiental, equipos, materiales y servicios para control de derrames y prevención de accidentes.

- ✓ Incrementar el volumen de crudo procesado a fin de aumentar los productos derivados, abastecer una mayor demanda y lograr mejores índices de eficiencia.

- ✓ Desarrollar programas de capacitación que contribuyan a la motivación y productividad del personal.

- ✓ Desarrollar programas de ayuda social y comunitaria.

3.1.4. **Descripción histórica de Petroindustrial.**

La Empresa Estatal de Industrialización de Petróleos del Ecuador: Petroindustrial es una de las filiales de la Empresa Estatal de Petróleos del Ecuador: Petroecuador, creada el 26 de diciembre de 1989, como parte del proceso de transformación empresarial de CEPE (Corporación Estatal Petrolera Ecuatoriana), con el siguiente objetivo:

"Óptima utilización de los hidrocarburos, que pertenecen al patrimonio inalienable e intangible del Estado, para el desarrollo económico y social del país, de acuerdo con la política nacional de hidrocarburos establecida por el Presidente de la República, incluyendo la investigación científica y la generación y transferencia de tecnología".

El holding empresarial de Petroecuador está conformado de la siguiente forma como se muestra en la Figura 3.1, donde se destaca la ubicación de Petroindustrial como la filial de refinación de crudo y producción de derivados de petróleo.

Además de Petroindustrial, Petrocomercial y Petroproducción, se muestran las demás Gerencias Administrativas y Operacionales que conforman la Estructura Organizacional de Petroecuador; así:

Gerencia de Economía y Finanzas.
Gerencia de Comercio Internacional.
Gerencia de Contratos
Procuraduría.
Gerencias de Medio Ambiente.
Gerencia Administrativa

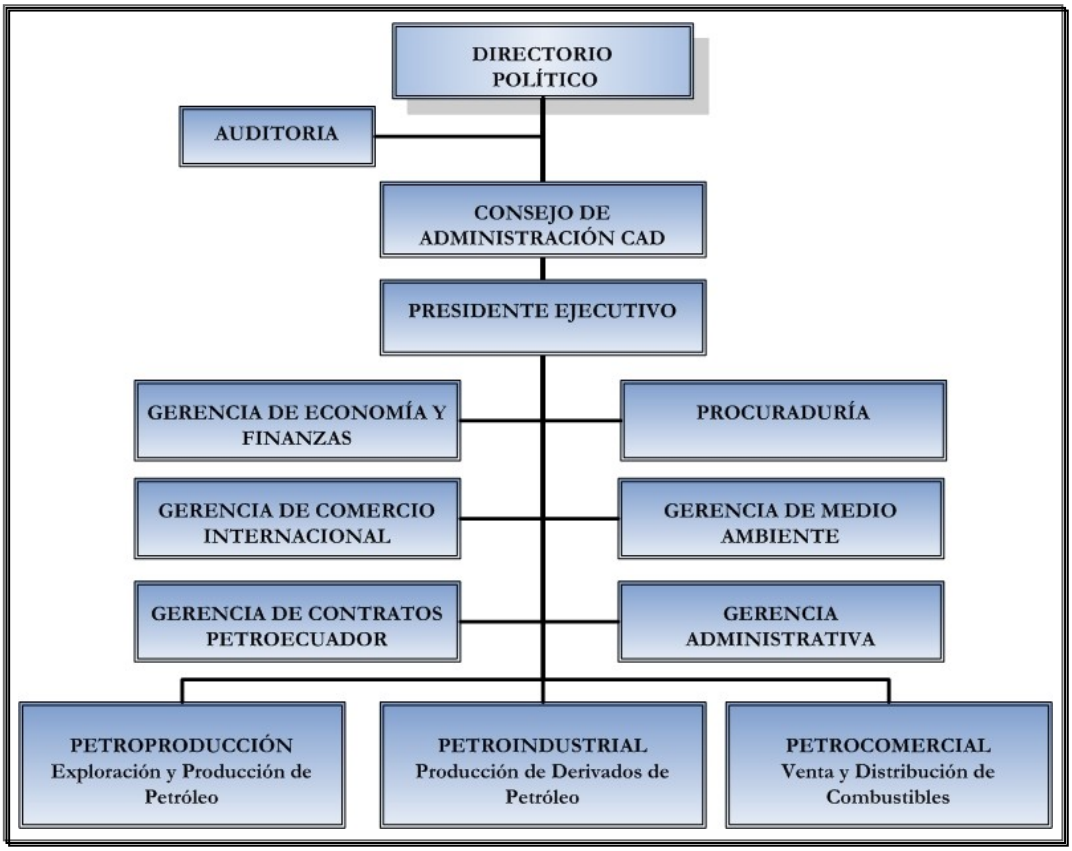


Fig.3.1: Ubicación de Petroindustrial dentro del Organigrama Estructural de Petroecuador
FUENTE: Informativo de la Gerencia de Economía y Finanzas de Petroecuador, Año 2002 No. 017

3.1.5. **Principal Actividad de Petroindustrial.**

Petroindustrial tiene como principal actividad fundamental la industrialización del petróleo existente en el país, así como también la administración de las plantas de industrialización instaladas dentro del territorio ecuatoriano.

Administra las siguientes plantas:

Refinería Estatal de Esmeraldas, la cual entró en funcionamiento en 1978 y cuya capacidad de refinación es de 110.000 barriles/días. (Datos para año 2004).

Complejo Industrial de Shushufindi, dentro del cual funciona una planta de gas criogénica con capacidad para procesar 25 MMPCD de gas natural, y una refinería con capacidad de 40.000 barriles/día.

Refinería La Libertad, aquí se disponen de dos refinerías, las cuales en la actualidad disponen de procesos de destilación atmosférica, cuya capacidad es de 45500 barriles/día.

Adicionalmente en la región oriental, Lago Agrio, existe también una refinería muy pequeña de 1000 barriles/día, la misma que cubre únicamente las necesidades de Petroamazonas.

Entonces, el objetivo fundamental de Petroindustrial es la administración de las plantas de industrialización de petróleo existentes en el país. Esto es, programar la producción de las plantas y controlar estrictamente su cumplimiento, haciendo operar las diferentes unidades de aquellas en su máxima capacidad en la mayor parte, sin dejar de lado las condiciones de operación.

3.1.6. **Objetivos de la automatización de la empresa.**

Consolidar la información de la producción de las refinerías de Petroindustrial en la matriz, con el objeto de que constituya una herramienta de apoyo en la toma de decisiones sobre la producción de derivados de petróleo en el país.

Generar, procesar y distribuir la información requerida para sustentar la toma de decisiones oportunas, económicamente factibles y consistentes para optimizar su gestión.

Estructurar e impulsar el nivel de tecnología de la empresa.

Tener sistemas de información que permita concentrar los datos que se obtiene de forma manual, como los que se obtienen automáticamente, y que se encuentran dispersos en todas las plantas procesadoras de petróleo a fin de que se constituya en una herramientas de apoyo que permita acceder oportunamente a la información precisa para elevar el nivel de gestión operativa y de control de los recursos industriales.

Tener la información que sea consistente, exacta, oportuna, económicamente factible y relevante sobre:

Control de Producción.
Stock de Productos.
Operación de las Instalaciones.
Control de Calidad
Administrativo, financiera y contable.

De manera que facilite la toma de decisiones acertadas sobre la industrialización del petróleo en el país.

Aligerar las actividades que realizan los ejecutivos y el personal, para facilitar toma de decisiones, sus tareas y mejorar su productividad. Así como también garantizar la integridad de los datos

Procesamiento ágil de información administrativa y financiera, así como el incorporar nuevos avances tecnológicos a la empresa.

3.2.LA UNIDAD DE SISTEMAS DENTRO DE LA FILIAL.

Como podemos observar en el organigrama, la Unidad de Sistemas en la empresa se encuentra ubicado a un nivel de Asesoría y depende directamente de la Vicepresidencia.

Dicha ubicación, facilita la gestión de recursos, ahorro de trámites y sobre todo la facilidad de que se cumplan las distintas sugerencias que emite. Dichos criterios que emite la Unidad se convierten en disposiciones luego de la aceptación de la Vicepresidencia, lo que facilita:

- ✓ Emitir normativas y procedimientos generales sobre los recursos informáticos.
- ✓ Mantener a la empresa con los recursos necesarios sin subestimarlos ni sobredimensionarlos.
- ✓ Contar con una política informática que se aplique a toda la filial.
- ✓ Implementar proyectos corporativos.
- ✓ Estandarizar marcas.

La no dependencia de otras Unidades, o departamentos intermedios facilitan la gestión y operación de la Unidad de Sistemas. En la Figura 3.2 se destaca la ubicación de la Unidad de Sistemas dentro de la estructura organizacional de Petroindustrial.

Organigrama Organizacional de Petroindustrial

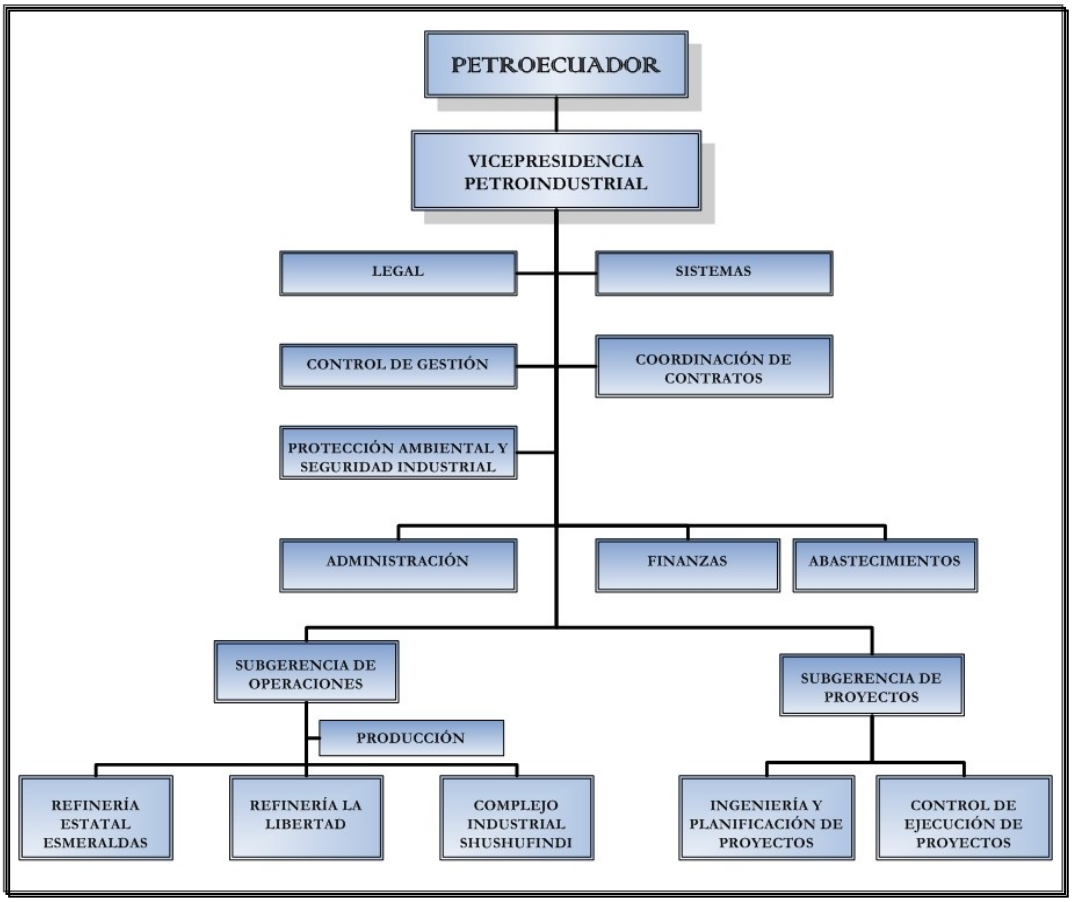


Fig.3.2: Ubicación de la Unidad de Sistemas dentro del Organigrama Estructural de Petroindustrial

FUENTE: Referencia [28].

3.2.1. **Misión**

La misión de la Unidad de Sistemas de Petroindustrial está definida como:

"Implementar soluciones informáticas que apoyen la gestión técnica y administrativa de la actividad de industrialización del petróleo."

3.2.2. **Objetivos de la Unidad de Sistemas.**[28]

- ✓ Implementar soluciones informáticas específicas para PETROINDUSTRIAL.

[28] Manual de Procedimientos y Funciones – Petroindustrial. Año 2005.

- ✓ Realizar el desarrollo, implantación y mantenimiento de sistemas y aplicaciones informáticas específicas y corporativas.

- ✓ Administrar los recursos informáticos de hardware y software de la Filial.

- ✓ Coordinar la obtención del servicio del sistema de telecomunicaciones de Petroecuador, para las cuatro Unidades Operativas de la Filial.

- ✓ Brindar soporte técnico a los funcionarios de todas las áreas de la empresa sobre el funcionamiento y utilización del software y hardware computacional.

3.2.3. **Análisis FODA.**

FACTORES INTERNOS:	
Fortalezas	**Debilidades.**
• Organización distribuida en 4 Unidades Operativas • Sólida plataforma de HW y SW corporativo • Personal Técnico especializado • Administración corporativa de recursos informáticos	• No se satisfacen las necesidades de información de PIN (Aéreas Técnicas) • Falta capacitación y acceso a tecnología actualizada • Fallas de comunicación y difusión con algunas áreas
FACTORES EXTERNOS:	
Oportunidades	**Amenazas**
• Necesidad de apoyo informático en áreas técnicas • Urgencia de incorporar tecnología moderna en procedimientos actuales • Requerimiento de integración hacia tecnología disponible en AREE	• Falta de inversión en proyectos tecnológicos que requiere Petroindustrial. • Contratación aislada de tecnología informática-falta de procedimientos • Personal informático en otras unidades

3.3.ESTRUCTURA Y FUNCIÓN DE LA UNIDAD DE SISTEMA.

La Unidad de Sistemas de PETROINDUSTRIAL Matriz, se encuentra trabajando bajo una administración basada en áreas operativas, las cuales obedecen a un nivel

Directivo denominado Jefatura. Todos los integrantes mantienen como soporte y asesoría a la Secretaría quien ayuda en los trámites internos y externos de la Unidad.

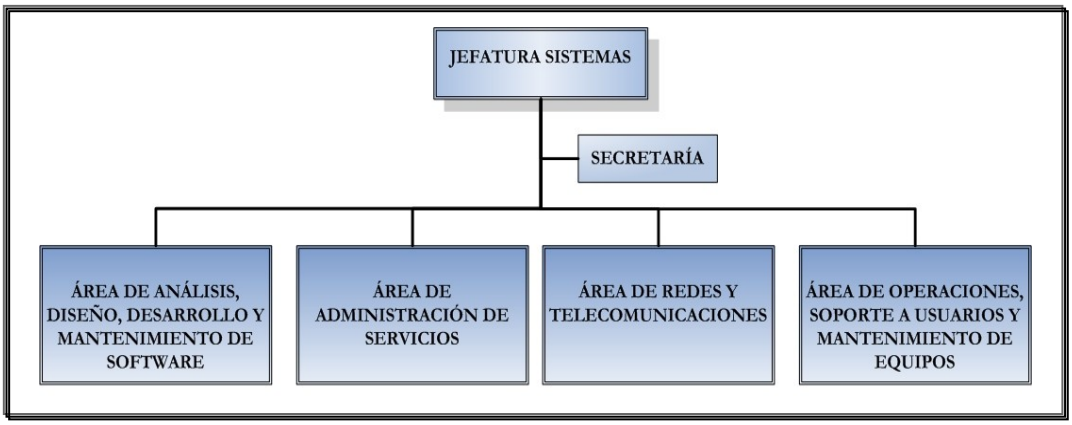


Fig.3.3: Organigrama Unidad de Sistemas Petroindustrial

FUENTE: Referencia [28].

La Jefatura es la responsable y representante de la Unidad ante los Niveles Directivos y Unidades Usuarias tanto en PETROINDUSTRIAL como en los Distritos, además también para entidades gubernamentales o no fuera de Petroecuador.

Se cuenta con el Área de Análisis, Diseño y Desarrollo de software que es la encargada del la generación y mantenimiento de los sistemas informáticos de la Matriz. Todo ello basado en una metodología de desarrollo hasta culminar con la capacitación y entrega de manuales de usuario y técnicos.

El Área de Administración y Servicios, donde se administran los servicios que están disponibles en la red, así como los sistemas ya culminados y que se encuentran en producción. Tienen a su cargo administración de Sistemas Operativos, Bases de Datos, Servicios de Internet, Correo electrónico, Antivirus, etc.

En el Área de Redes y Comunicaciones se realiza toda la administración, configuración, mantenimiento de las redes LAN y WAN de la Matriz. Se establece las seguridades a nivel de red y también se cuenta con la Administración y Operación de los Servidores AS/400.

El Área de Operaciones, Soporte a Usuarios y Mantenimiento de Equipos, se encarga de administrar el licenciamiento del software así como las instalaciones, en hardware garantías, mantenimientos y actualizaciones. En esta área se mantiene el Help Desk al usuario final.

Las Áreas dependen de la Jefatura y se coordina el trabajo en base a objetivos trimestrales y anuales, con informes mensuales de cada Área hacia la Jefatura. De igual forma los proyectos de inversión son generados en cada área, abalizados y tramitados por la Jefatura hacia los niveles Directivos.

CAPITULO IV

TECNOLOGÍAS UTILIZADAS Y PROYECTADAS EN PETROINDUSTRIAL

4.1. Tecnologías utilizadas en Petroindustrial.

4.2. Tecnologías proyectadas en Petroindustrial.

4.3. Características, Ventajas y Desventajas.

4. TECNOLOGÍAS UTILIZADAS Y PROYECTADAS EN PETROINDUSTRIAL

Petroindustrial, como una más de las empresas que depende día a día de la información, para la toma de decisiones respecto del funcionamiento de sus plantas de refinación de crudo; tiene actualmente a su disposición tecnología de punta en el área de redes y telecomunicaciones instalada en sus 3 Refinerías a nivel nacional, pero no por esto está exenta de planificar mejoras y actualizaciones de dicha tecnología con el fin de mantener y elevar la calidad de sus medios de comunicación y transporte de información.

Es por este motivo que, en este capítulo describiremos las tecnologías que actualmente Petroindustrial tiene montadas en su infraestructura de Redes y Telecomunicaciones, analizando cuales serían las mejores alternativas de mejoramiento que podrían aplicarse, para mantener la calidad de los servicios ofrecidos para el completo desenvolvimiento de las actividades de la empresa.

4.1.TECNOLOGÍAS UTILIZADAS EN PETROINDUSTRIAL.

Dentro de la infraestructura tecnológica que Petroindustrial tiene implementada en sus instalaciones tanto en Matriz – Quito, como en sus tres Refinerías podemos destacar las siguientes:

Petroindustrial Matriz – Quito:

A nivel del edificio Matriz – Plaza LAVI, en la ciudad de Quito, el mismo que dispone de 12 pisos de construcción, cuenta con una instalación de cableado estructurado completamente nuevo tanto a nivel horizontal como vertical. A nivel de pisos, es decir, el cableado horizontal es Categoría 6 para la red de datos y voz, la misma que cumple con las normas internacionales EIA/TIA de instalación, con el fin de brindar a sus usuarios las mejores prestaciones y un alto rendimiento a nivel de red LAN.

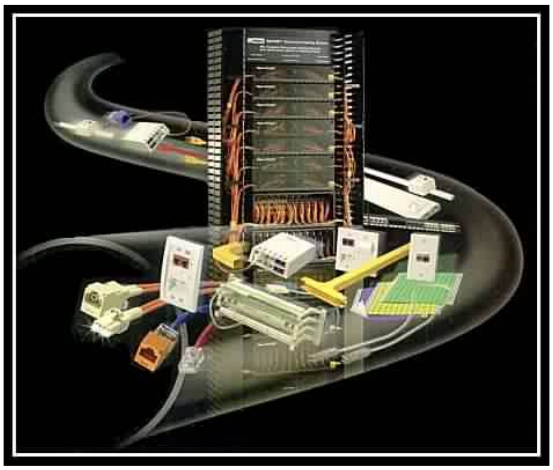


Fig: 4.1: Componentes del Cableado Estructurado
FUENTE: Cableado Estructurado. Electrónica LAM.: http://hermosillovirtual.com/lam/cableado.htm. 2005-05-13.

Para brindar un óptimo desempeño de la red LAN se ha instalado cada 2 pisos dentro del edificio un RACK de pared con su respectivo Equipo Activo de Red, llegando a ser un total de 5 Racks más 2 Armarios Racks Principales dentro del DATA CENTER ubicado en el piso 8 correspondiente a la Unidad de Sistemas. Cada Rack ha sido ubicado y diseñado para cubrir todos los puntos de datos y voz instalados en los dos pisos a los que brinda servicio.

Fig: 4.2: Rack de Piso y Equipo Switch de Red
FUENTE: Cableado Estructurado. Electrónica LAM.: http://hermosillovirtual.com/lam/cableado.htm. 2005-05-13.

El Backbone vertical instalado en el edificio Matriz de Petroindustrial para unir los 5 racks de piso con el armario principal dentro del Data Center de Sistemas es de fibra óptica multimodo el cual cuenta con una línea principal de servicio y una de backup. Esta instalación también cumple con las normas internacionales a fin de ofrecer el más alto rendimiento y nivel de crecimiento a nivel de red.

Fig: 4.3: Switch Cisco Catalyst 3560G Capa 3
FUENTE: Cisco Systems Latinoamérica - Redacción Virtual: http://ciscoredaccionvirtual.com/redaccion/articulodestacado/ver_comunicados.asp?Id=570. Año 2006.

Como se mencionó antes en cada Rack de Piso se tiene instalado un equipo de red activo de marca Cisco System de la serie Catalyst 3560G de Capa 3, que dispone de 48 puertos gigabit ethernet (10/100/1000MB) más 4 puertos Uplink de Fibra.

Estos equipos están conectados mediante fibra óptica un equipo principal de red, el mismo que es un Switch-Router de marca Cisco System de la serie 4500 de Capa 3, el cual dispone de 192 puertos gigabit ethernet más 8 puertos uplink de fibra óptica. Este equipo principal se encuentra instalado en el Armario Rack Principal dentro de Data Center de la Unidad de Sistemas y cumple la función de Switch de Core o núcleo de la red LAN de Petroindustrial.

Fig: 4.4: Router Motorola Vanguard 6455
FUENTE: TGS: Vanguard Router Solutions: http://www.tgscorp.com/vanguard.php. Año 2006.

A nivel de equipos de enrutamiento o Ruteadores, y con el fin de proporcionar un ancho de banda adecuado para mantener la comunicación estable con sus tres refinerías, Petroindustrial tiene instalado a nivel nacional equipos ruteadores Motorola- Vanguard modelo 6455, en los cuales tiene habilitada la tecnología de encapsulamiento Frame Relay. Estos equipos además tienen el soporte para encapsulamiento de voz a través de

tarjetas FXS y FXO, lo que proporciona conectividad tanto a nivel de datos como de voz con las refinerías.

Un detalle más que es importante recalcar de estos equipos de enrutamiento Vanguard es la disponibilidad de una tarjeta con soporte para enlaces E1 a 2048 Bytes por segundo, la misma que está prestando servicio y operando en condiciones normales y permitiendo enviar por este medio hasta 30 canales de voz al mismo tiempo.

De la misma forma, Petroindustrial dispone de una central telefónica marca NEC modelo IP NEAX 2000, la cual integra 3 tarjetas E1 para comunicaciones, de las cuales solamente 1 de las tarjetas se encuentra habilitada y sincronizada con el equipo principal de enrutamiento Router Vanguard 6455, por medio de la cual se está enviando un total de 14 extensiones telefónicas distribuidas a los tres campos de refinamiento a nivel nacional.

Fig: 4.5: Central Telefónica NEC IP NEAX 2000

FUENTE: NEC DE COLOMBIA:
http://www.nec.com.co/productos/pbx_neax2.htm. 2006-01-17

Petroindustrial Refinerías:

A nivel de infraestructura en las instalaciones de refinamiento de crudo a nivel nacional, se dispone dentro de cada campo, de cableado estructurado categoría 5E al interior de los edificios, además para los enlaces largos, se dispone de conexiones a través de fibra óptica y también de enlaces Wireless o de radio según sea la necesidad. Dentro de los equipos activos de red, las refinerías cuentan con equipos de marca Cisco System de las series 2900, 3500 y 3700, tanto de capa 2 como de capa 3; así como también de equipos de marca 3COM con puertos fast-ethernet (10/100Mb) y gigabyte-ethernet (10/100/1000Mb). Estos equipos brindan la conectividad, ancho de banda y performace

necesario para las operaciones correctas de las instalaciones de las refinerías de Petroindustrial.

Fig: 4.6: Equipos activos de Red LAN

FUENTE: Cisco Announces the Catalyst 4500 Series News@Cisco: http://newsroom.cisco.com/dlls/prod_091702.html. Año 2006.

4.2.TECNOLOGÍAS PROYECTADAS EN PETROINDUSTRIAL.

La Unidad de Sistemas de Petroindustrial Matriz, tiene algunos proyectos tecnológicos de mejoramiento y actualización dentro su infraestructura, tanto a nivel de red LAN como WAN, los mismos que se detallan a continuación:

4.2.1. **Rediseño de la Red LAN de Petroindustrial Matriz y Refinerías.**

Proyecto tecnológico de primordial importancia que se ha planteado la Unidad de Sistemas, es la reestructuración de toda la red LAN tanto de Petroindustrial Matriz como de las tres refinerías, dado que al momento y por el crecimiento del parque informático de la empresa, especialmente a nivel de la matriz, el actual sistema de direccionamiento IP a nivel de red LAN se encuentra en estado crítico. Esto implica que el número de direcciones IP de los rangos establecidos en las VLAN's de la red está a punto de terminarse. Este proyecto actualmente se encuentra en la fase de recolección de datos, con el fin de obtener una imagen clara de la actual infraestructura tecnológica que dispone Petroindustrial y dado que su alcance involucra tanto a la Matriz, como a sus refinerías; es de alto énfasis el llegar a obtener los mejores resultados de análisis y aplicación de este proyecto.

4.2.2. **Reemplazo de Equipos de Enrutamiento del Sistema Integrado de Telecomunicaciones.**

Proyecto tecnológico planteado a nivel de redes y telecomunicaciones, es el estudio técnico para el reemplazo de los equipos de enrutamiento instalados a nivel nacional Marca Motorola Vanguard, con tecnología de encapsulamiento Frame Relay por otros de Marca CISCO, que cumplan las misma funcionalidades y además permitan elevar el ancho de banda de los enlaces que Petroindustrial mantiene con sus tres refinerías en todo el país permitiendo incorporar tecnologías como ATM para la trasmisión de datos. Este proyecto se encuentra en la fase de conversaciones con el personal técnico de Petrocomercial, dado que la Unidad de Redes y Telecomunicaciones de esta filial de Petroecuador, es la encargada de la administración de todo el sistema integrado de telecomunicaciones y Petroindustrial mantiene un convenio de colaboración tecnológica con la misma.

4.2.3. **Implementación de Enlaces E1 con todas las Refinerías.**

Proyecto de gran importancia y que va encaminado a mejorar directamente el ancho de banda de los enlaces de telecomunicaciones con cada Refinería de Petroindustrial; es la implementación de enlaces directos E1, los mismos que serían implementados una vez que Petrocomercial, que es la filial, encargada de la administración del sistema nacional de telecomunicaciones, termine la instalación y acondicionamiento de los equipos e infraestructura necesaria para este propósito. La instalación de estos enlaces viene incluida como parte del convenio de telecomunicaciones establecido y firmado por las dos filiales.

4.2.4. **Instalación de Equipos Firewall de Seguridad.**

Con el objetivo de mejorar las seguridades existentes dentro de la red, se ha puesto en marcha el proyecto instalación de un equipo Firewall perimetral para la protección de la información de la empresa, prevenir ataques ó robos de datos y caídas de los sistemas que puedan causar daño a la empresa en diario desempeño. Este proyecto se encuentra en la fase de estudio, esperando poner en marcha un prototipo para obtener resultados, que permitan evaluar y medir las necesidades de protección que deberán ser implementadas a nivel del proyecto final.

4.2.5. **Implementación de Sistema de Video Conferencia con Refinerías.**

Aprovechando la infraestructura tecnológica actual que posee Petroindustrial se ha planteado el proyecto de implementación de un sistema de video conferencia entre la Matriz de Petroindustrial y las 3 refinerías, con el objetivo de mejorar el desarrollo de actividades administrativas y de control, ya que las mismas se ven retrasadas por el múltiple papeleo que involucran, pudiendo por este medio tecnológico ser desempeñadas de mejor manera, ya que la comunicación y la toma de decisiones sería mucho más rápida. Actualmente este proyecto se encuentra en la etapa de aprobación para salir a concurso público tal como lo establece el reglamento de proyectos de Petroindustrial.

4.2.6. **Renovación, actualización y consolidación de Servidores de Red.**

Además de los proyectos de redes, hay otro proyecto tecnológico enfocado en el mejoramiento del sistema de servidores de administración, que indirectamente va relacionado con el desempeño de la red LAN y WAN de Petroindustrial. Este proyecto involucra el reemplazo de los equipos servidores de mesa por servidores Blade de Rack, lo que incorpora también la actualización de los sistemas operativos y la migración de los servicios de red, con el fin de obtener el mejor rendimiento y performance a nivel de la red LAN. Actualmente este proyecto está en la fase de aprobación para la compra por parte de la Procuraduría General del Estado que es la entidad de control, que emite los informes favorables para proyectos que involucran un elevado presupuesto de inversión como es en este caso.

4.3.CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS.

Dentro del estudio para la implementación de los proyectos tecnológicos proyectados por la Unidad de Sistemas de Petroindustrial dentro del área informática, se establecen las siguientes características, las mismas que se detallan a continuación:

4.3.1. **Rediseño de la Red LAN de Petroindustrial Matriz y Refinerías.**

Este proyecto tiene como objetivo y característica principal el mejorar la estructura lógica de la red LAN del edificio matriz, permitiendo tener un mayor número de direcciones IP asignables para hosts dentro de las Vlan’s o subredes.

Implementar la estructura más adecuada de red para cada una de las instalaciones físicas que tienen las refinerías y acorde con su estructura organizacional.

Mantener un esquema de direccionamiento adecuado y acorde con la distribución física de las unidades y equipos de computación dentro del nuevo edificio.

Mejorar el nivel de los servicios ofrecidos por la Red LAN e identificar los cuellos de botella causantes del exceso de tráfico dentro de la red.

Establecer la configuración lógica adecuada para cada equipo activo de red dentro del edificio, con el objetivo de obtener el mejor rendimiento y performace de dichos equipos, además adecuar soporte de backup en caso de que se presenten falla que ocasiones caídas del servicio de red.

4.3.2. **Reemplazo de Equipos de Enrutamiento del Sistema Integrado de Telecomunicaciones.**

Dentro de este proyecto el objetivo principal es elevar el ancho de banda de los canales de comunicación, estandarizando tecnologías y marcas a nivel de toda la red tanto LAN como WAN de Petroindustrial.

Se pretende implementar nuevas tecnologías de empaquetamiento de datos con el fin de mejorar los servicios ofrecidos por la red actual, tanto a nivel de voz como de datos.

Permitir la integración a nivel nacional de las centrales telefónicas PBX a través del sistema integrado de telecomunicaciones, elevando así el número de canales de comunicación entre Petroindustrial Matriz y sus Refinerías.

4.3.3. **Implementación de Enlaces E1 con todas las Refinerías.**

El desarrollo de este proyecto va enfocado a mejorar el camino de comunicación entre Petroindustrial Matriz y sus Refinerías, el cual al terminar la instalación de los Enlaces E1 con 2048 Kbps como ancho de banda, permitirá no solo una mejor fluidez de la comunicación digital, sino también ayudara en el desarrollo de proyectos que ocupan un elevado nivel de ancho de banda.

También viene involucrado como parte de este proyecto el habilitar un enlace confiable entre Matriz y Refinería La Libertad, ya que el enlace actual sufre constantes cortes por causas eléctricas y climáticas, lo que afecta el normal desempeño y operatividad de las comunicaciones, causando retrasos en el envío de información y actualización de la misma para la toma de decisiones.

Este proyecto es una base para los proyectos de integración de las centrales telefónicas PBX a nivel nacional y además permitirá la implementación del proyecto de Video conferencia, el mismo que, en sus características de instalación, especifica que para un óptimo funcionamiento de dicho sistema de comunicación se recomienda elevar el ancho de banda actual del enlace que se mantiene con cada una de las refinerías.

4.3.4. **Instalación de Equipos Firewall de Seguridad.**

Dentro de los proyectos prioritarios a nivel de red LAN en Petroindustrial Matriz se encuentra la implementación, instalación y adecuada configuración de un equipo Firewall (Cortafuegos), con el fin de brindar a toda la red de datos la seguridad necesaria ante intrusos, fallos y potenciales ataques que atenten contra la integridad de la información manejada a nivel institucional.

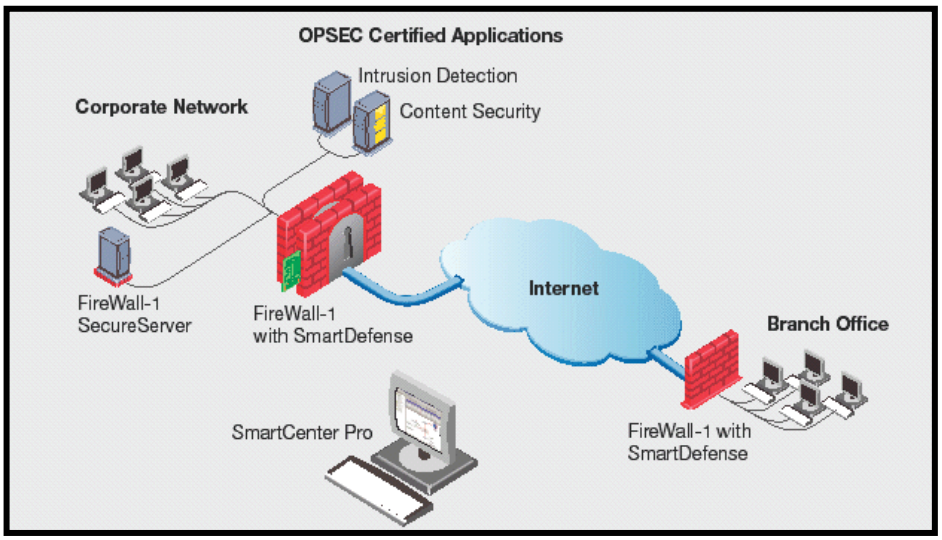


Fig: 4.7: Diagrama de protección con Firewalls

FUENTE: OptiCom - IT Infrastructure Solutions: FireWall-1: http://www.opticom.lv/en/products/security/firewall/checkpoint/cp1/. Año 2006.

El equipo a instalarse deberá cumplir con todos los estándares y niveles de protección especificados en el resultado del estudio que se realice del proyecto para la implementación de este dispositivo de seguridad, permitiendo así; implantar a la medida de la red de Petroindustrial las debidas protecciones y seguridades para un óptimo desempeño de la infraestructura tecnológica que se posee.

Siendo un firewall o cortafuegos, un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o

prohibiéndolas según las políticas de red que haya definido el área responsable de la red. El estudio de implementación deberá arrojar las características adecuadas para su modo de funcionar dentro de la red de Petroindustrial, acogiéndose a las sugeridas por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad.

En la siguiente figura se especifica la ubicación donde se planea instalar un firewall perimetral para proteger y controlar la red tanto interna como externa de Petroindustrial.

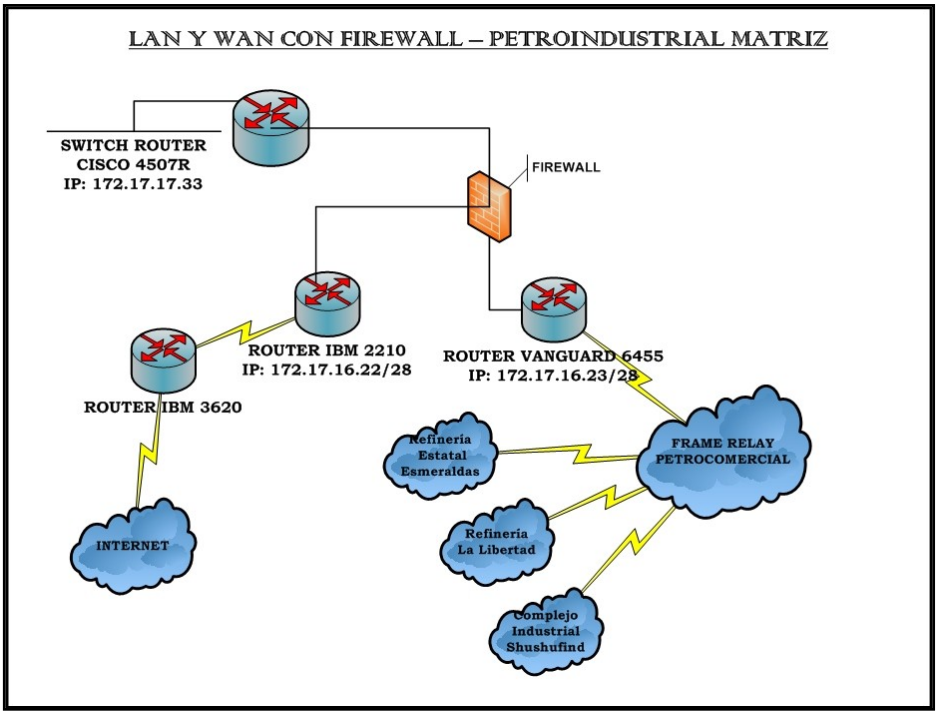


Fig: 4.8: Diagrama LAN Y WAN con protección de Firewall
FUENTE: Propio

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, es decir la red LAN con la red de Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna y pongan en peligro la información confidencial de la empresa.

4.3.5. **Implementación de Sistema de Video Conferencia con Refinerías.**

Con el fin de mejorar y elevar la calidad las actividades administrativas y de control a nivel de todo el sistema de Petroindustrial, se ha planteado la implementación de un sistema de video conferencia a nivel nacional el cual enlazaría las tres Refinerías y la

Matriz. Siendo la zona cero el edificio de Petroindustrial en la ciudad de Quito, se utilizaría el sistema de telecomunicaciones actual para poder acceder a las demás zonas remotas instaladas cada una en cada refinería, así el sistema de video conferencia estaría estructurado por un equipo principal y tres equipos remotos.

El ancho de banda requerido como mínimo por este sistema es 256 kbps y el ancho de banda ideal es de 512 kbps, por lo que este proyecto depende del mejoramiento del ancho de banda de los enlaces de telecomunicaciones actuales que se tiene instalados con cada uno de los distritos. La tecnología involucrada en este sistema de video conferencia es de última generación, por lo que será un proyecto tecnológico innovador a nivel nacional dentro de todas las filiales de Petroecuador.

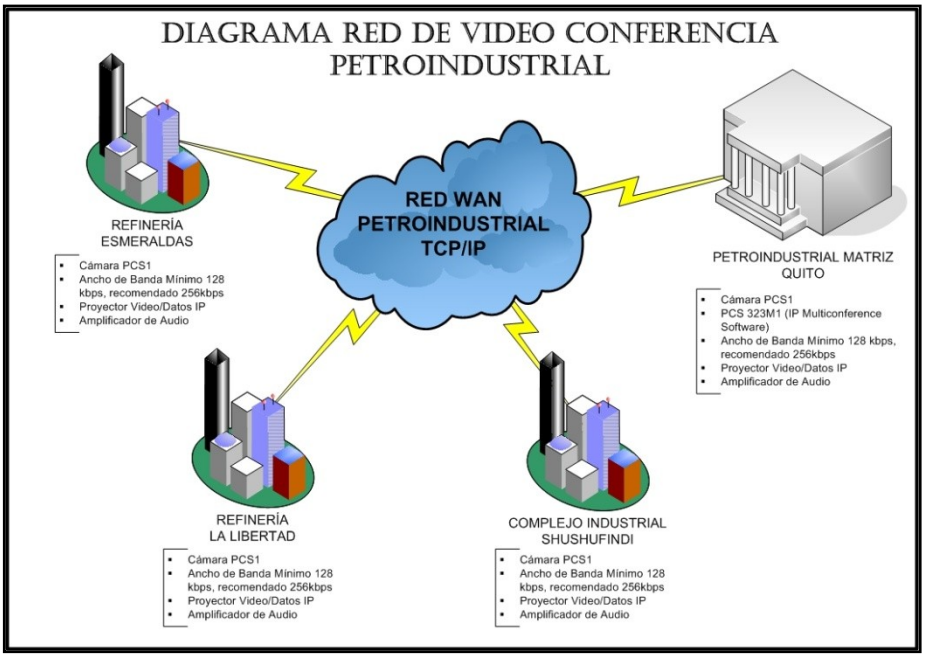


Fig: 4.9: Diagrama Red de Video Conferencia en Petroindustrial

FUENTE: Propio

El sistema de video conferencia incorpora tanto en equipos como en accesorios los siguientes componentes: software para habilitar video conferencia de acuerdo al equipo; 4 unidades de transmisión de datos, 1 principal y 3 remotas; 4 proyectores de video, 4 pantalla interactivas SMARTBOARD; y, 4 sistemas de audio en circuito cerrado. Todo esto con el objetivo de brindar la mejor calidad en este nuevo medio tecnológico de comunicación.

4.3.6. **Renovación, actualización y consolidación de Servidores de Red.**

Este proyecto tecnológico tiene como objetivo, realizar la renovación del parque de servidores que posee la unidad de sistemas y que brindan los servicios de DNS, MAIL, Base de Datos SQL y Administración Electrónica de Documentos.

Se incluye también la actualización y migración de servicios a la plataforma Windows 2003 Server, lo que vendrá a renovar las funcionalidades de las aplicaciones ofrecidas por los servidores que actualmente están prestando servicio. Con esta actualización se pretende también implementar la consolidación de servidores, llevándonos al camino de los servidores Blade, que son equipos que economizan espacio, y están diseñados para prestar un alto rendimiento y elevadas prestaciones a un bajo costo.

Esta consolidación es una tendencia tecnológica a la que están llegando muchas empresas, como las proveedoras de servicios de Internet y Petroindustrial no se quiere quedar atrás. Muchas son las ventajas de implementar las consolidación con servidores Blade, pues sus características, potencia de rendimiento, alta disponibilidad, manejo de recursos, bajo consumo de energía, eliminación por completo de cableado y bajo espacio utilizado (6 U de rack) los hacen muy adecuados para el objetivo planteado. Se puede tener instalado hasta 16 servidores Blade en el mismo espacio donde caben 4 servidores de mesa.

De igual manera la tecnología utilizada por este tipo de servidores es de última generación, lo que proporciona una calidad extraordinaria en cada componente. Su característica principal es que son como cuchillas que poseen únicamente la placa madre, la memoria RAM, el disco duro y los buses de datos. Los demás componentes como fuente de poder, CD-ROM, floppy, tarjetas de red, puertos de teclado, mouse, pantalla, y adicionales están ubicados en el chasis, de esta manera se realiza una consolidación efectiva compartiendo recursos sin de dejar de prestar un óptimo rendimiento. De igual manera la administración de los recursos compartidos es muy eficiente y se realiza desde una consola centralizada especialmente diseñada para este propósito.

CAPITULO V

ESTUDIO DE LA ESTRUCTURA Y PROBLEMAS DE RED DE PETROINDUSTRIAL

5.1. Estructura de la red LAN y WAN.

5.2. Características de la red y su configuración.

5.3. Identificación de principales problemas en la red.

5.4. Cuellos de Botella

5. ESTUDIO DE LA ESTRUCTURA Y PROBLEMAS DE RED DE PETROINDUSTRIAL

5.1.ESTRUCTURA DE LA RED LAN Y WAN.

La red LAN y WAN de Petroindustrial tiene una composición estructural con un elevado grado de complejidad, ya que ésta, como toda red actual, no está exenta de crecimiento y constantes nuevos requerimientos para satisfacer no solo las necesidades del área de sistemas, sino también las de los usuarios y las nuevas exigencias tecnológicas que sobre la red van imponiendo cada proyecto de innovación que se desarrolla dentro de esta filial de Petroecuador.

Actualmente la estructura de la red LAN de Petroindustrial en su nivel físico tiene la siguiente composición:

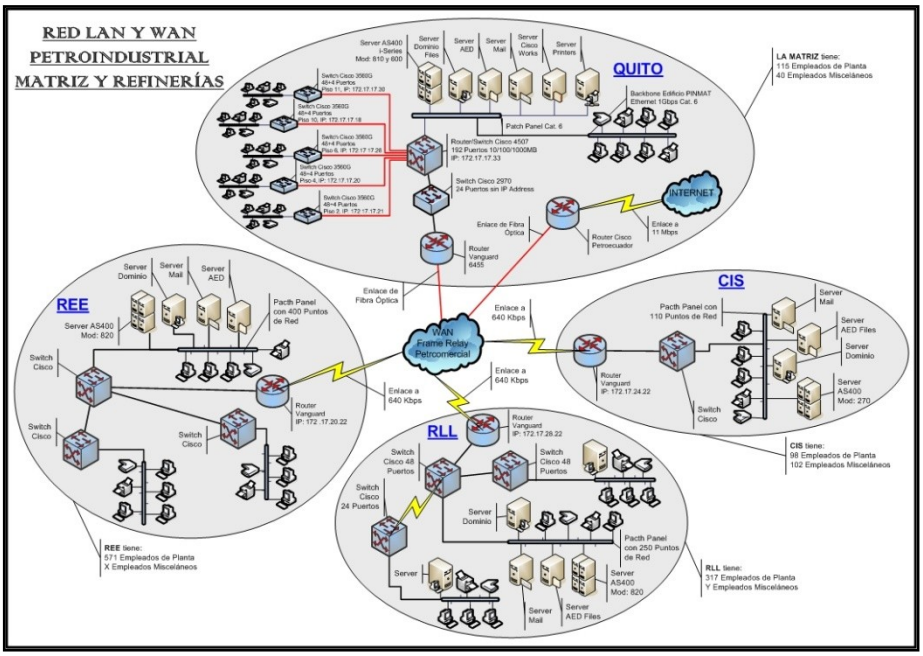


Fig: 5.1: Diagrama LAN-WAN de Petroindustrial

FUENTE: Propio

Como equipo activo de red principal o switch de core (núcleo) posee un Switch – Route de capa 3, marca Cisco System, modelo Catalyst de la serie 4507; el mismo que tiene instalado 4 módulos de 48 puertos gigabit ethernet y un módulo adicional de 6 puertos GBIC para conexiones up-link de fibra óptica.

Dentro del backbone vertical de fibra óptica tiene conectado 5 equipos switch de marca Cisco, modelo Catalyst de la serie 3500 con 48 puertos gigabit ethernet más 4 puertos up-link de fibra óptica que complementan su estructura.

Como equipo principal de enrutamiento tanto para la red LAN como WAN tiene un Ruteador Vanguard 6455 de marca Motorola, el mismo que cumple con la función de enlace entre las redes de las refinerías, a través del sistema de telecomunicaciones y la red de la Matriz de Petroindustrial. De la misma manera permite la conexión con la red de sistemas de Petroecuador, que es el área encargada de brindar el acceso a la red de Internet para toda la red LAN y WAN de Petroindustrial.

La estructura de la red LAN de Petroindustrial en su nivel lógico y de configuración tiene la siguiente composición:

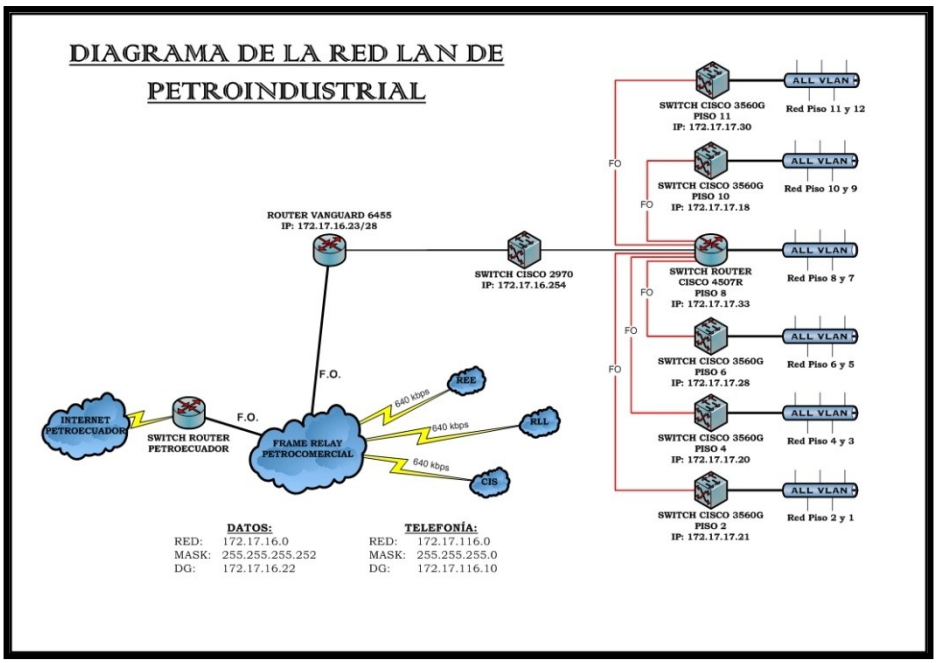


Fig: 5.2: Diagrama LAN de Petroindustrial Matriz

FUENTE: Propio

Para el sistema de direccionamiento actual se ha tomado como dirección de red LAN una de clase B, dentro de la cual se ha configurado subredes. En el equipo Switch Cisco Catalyst 4507 se tiene configurado un número de 10 Vlan's sobre la dirección de red manejada, con el objetivo de reunir a los usuarios y hosts en grupos de red administrables y más manejables; reduciendo así el broadcast. La distribución de las Vlan's se ha realizando ubicando la agrupación de acuerdo a la unidad de trabajo u oficinas que funcionan en cada uno de los pisos del edificio de Petroindustrial.

De las 10 Vlan's configuradas, la Vlan número 2, 9 y 10 tienen una máscara de 24 bits lo que proporciona un número de 254 direcciones IP asignables. La Vlan 2 esta asignada exclusivamente para la red de servidores e impresoras con puertos ethernet. La Vlan 9 se ha designado para la red de telefonía IP. Y por último la Vlan 10 se ha asignado como la Vlan de Seguridad que es donde se ingresan los PC's que por algún motivo están generado tráfico dentro de la red para su revisión y corrección del problema.

El resto de Subredes ó Vlan's de este esquema actual de direccionamiento tiene un rango de 32 direcciones IP, siendo asignables un total de 30 direcciones para los host; rango que actualmente es insuficiente para cubrir el número de host que deben estar conectados a ciertas Vlan's. A parte de toda la configuración de Vlan's dentro del equipo Switch Cisco, también se ha incorporado una tabla de rutas para que el tráfico sea correctamente direccionado hacia el próximo salto a donde pertenece. Aquí están incluidas las rutas que dirigen el tráfico tanto para cada una de las redes de las refinerías, así como también el tráfico que va hacia la red de sistemas de Petroecuador para la salida a Internet.

A nivel de la red LAN de las refinerías de Petroindustrial no se viene manejando ningún tipo de agrupamiento por Vlan's o subredes, únicamente se tiene configurada una red de clase B con máscara de 24 bits, que proporciona 254 direcciones IP asignables, lo que provoca una zona enorme de broadcast generando gran cantidad de tráfico dentro de dicha red. A esto se suma también la falta de control sobre el tipo de tráfico con que inundan los host la red.

5.2.CARACTERÍSTICAS DE LA RED Y SU CONFIGURACIÓN.

Como características principales de la Red LAN y WAN de Petroindustrial describiremos las siguientes:

- El esquema de direccionamiento está basado en una red de clase B. (172.*.*.*), con el fin de poder permitir crecimiento y adaptabilidad a los cambios tecnológicos.

- Se mantiene la implementación y administración de subneting (subredes, vlan's) para reducción de zonas de broadcast y mejor control de los grupos de usuarios dentro de la red.

- La distribución de las Subredes o agrupaciones de hosts está desarrollada de acuerdo a la ubicación de las unidades u oficinas dentro del edificio de Petroindustrial.

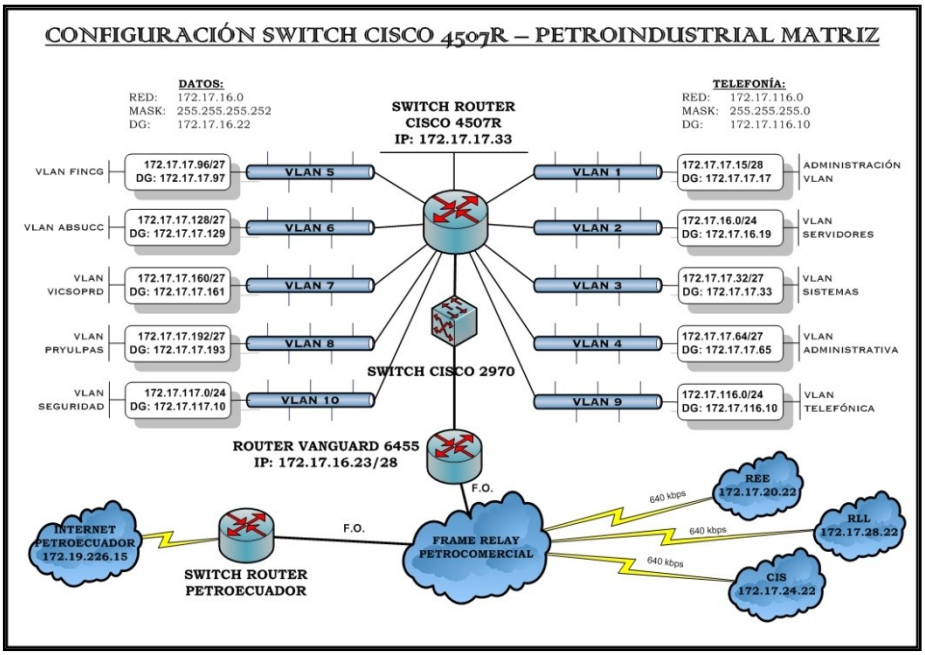


Fig: 5.3: Configuración VLAN's Petroindustrial Matriz

FUENTE: Propio

- Se ha implementado la configuración de una Vlan de Servidores en la que se incluyen también las impresoras de red. Esta Vlan tiene una máscara de 24 bits, proporcionando 254 direcciones IP asignables, pero todas las direcciones IP asignadas de este segmento de red son establecidas como fijas lo que permite tener un mayor control administrativo.

- Para el correcto funcionamiento de la telefonía IP, se ha configuración una Vlan exclusiva para este propósito, permitiendo de este modo controlar el broadcast provocado por las comunicaciones de la Telefonía IP dentro de este segmento de red.

- En cada uno de los distritos de Petroindustrial, es decir en cada refinería se tiene configurado a nivel del switch principal dominios VTP con el fin de controlar la propagación correcta de la configuración de las Vlan's a los demás switches de la red.

- Con el fin de establecer una zona de seguridad se mantiene la configuración de una Vlan para Seguridad, para equipos que presentan problemas, generando demasiado tráfico no justificado dentro de una red o para equipos que se

encuentran en tránsito, con el fin de proporcionar seguridad a los demás segmentos de la red.

- Se tiene definido una tabla de enrutamiento para tráfico de red, tanto para el interno, es decir, el tráfico desde la matriz de Petroindustrial hacia las refinerías; así como también para el tráfico hacia Internet, el cual es proporcionado desde la red de Petroecuador a través de un proxy.

- Dentro de la configuración lógica de las interfaces físicas de fibra óptica, estás se encuentran en modo TRUNK, lo cual permite la propagación de la configuración de Vlan's desde el equipo switch de core hacia los switches clientes de cada piso.

- Configuración del enrutamiento de la red WAN hacia las redes LAN de refinerías aplicada dentro de las tablas de rutas del equipo Vanguard Morola 6455.

- Implementación de rutas dentro de la configuración de enrutamiento de los equipos de la red tanto LAN como WAN de Petroindustrial, para permitir el acceso de ciertos equipos del Ministerio de Energía y Minas y la Dirección Nacional de Hidrocarburos (Organismos de Control del Estado) hacia los servidores de base de datos de las refinerías con el fin de hacer las consultas de información acerca de la operación y producción diaria de derivados de petróleo.

- Sistema de telefonía IP implementada dentro de la configuración de la red, integrando la central telefónica híbrida marca NEC modelo Neax 2000 con los equipos switch Cisco.

- Configuración de canales para el envío de voz a través de tarjetas FXO y FXS instaladas en los equipos ruteadores Vanguard a nivel de toda la estructura de la red WAN de Petroindustrial.

- Configuración de canal de comunicaciones E1 para el envío de extensiones y líneas telefónicas, a través del sistema integrado de telecomunicaciones entre centrales telefónicas.

5.3.IDENTIFICACIÓN DE PRINCIPALES PROBLEMAS EN LA RED.

En las condiciones descritas anteriormente para la red de Petroindustrial, vale señalar que hay problemas que saltan a la vista con mucha facilidad, en cambio hay otros que

están inmersos o dependientes de otros factores asociados a los niveles de servicio que presta la red a todos sus usuarios.

Dentro de los principales problemas de red identificados dentro de la LAN de Petroindustrial Matriz podemos señalar los siguientes.

- Rango de direccionamiento IP dentro de las Vlans muy corto para el número actual de usuarios por cada unos de los segmentos de red. Especialmente en ciertas Vlans donde se agrupan unidades con muchos equipos PC's.

- No existe control de tráfico de red a ningún nivel, excepto por el proxy de Petroecuador que de alguna forma filtra el acceso a los recursos e información ofrecidos por la Internet.

- Sistema de protección antivirus corporativo utilizando una versión antigua que no está acorde con las exigencias de seguridad solicitadas hoy en día. Además el uso de este antivirus en equipos con sistema Windows 98, ocasiona no solo lentitud en estos equipos, sino que provoca una incidencia bastante preocupante dentro del comportamiento de la red. Puesto que al ser un numero grande de equipos con este sistema operativo, ocasiona que los servicios ofrecidos por la red LAN y consumidos por estos equipos sufran un elevado índice de errores, debido tanto a la vetustez de los equipos así como, del Software Base que funciona en ellos.

- No existe sistema de protección perimetral o firewall ni a nivel interno ni externo, por lo que la información de Petroindustrial y la red LAN puede estar expuesta a inminentes ataques o atacantes externos e internos. Este problema unido a la falta de monitoreo pone en peligro inminente la seguridad de la información.

- Políticas de uso de recursos de red no establecidos para ningún usuario. Únicamente se tiene aplicadas las políticas normales que vienen disponibles en Active Directory de Windows 2000, pero que no involucran mayor control sobre el consumo de recursos de la red LAN.

- No existe sistema de actualizaciones para sistemas operativos, lo que provoca que los equipos estén expuestos a fallas de seguridad por la falta de estos updates (parches o service packs). Este problema es sumamente grave, ya que sumado al problema de utilizar una versión antigua de antivirus eleva las vulnerabilidades de la red.

Dentro de los principales problemas de red identificados dentro de la LAN de Petroindustrial Refinerías podemos señalar los siguientes.

- No existe un adecuado sistema de direccionamiento IP dentro de la red LAN de cada refinería y tampoco se maneja configuración de Vlan's. Esto ocasiona una zona muy grande de broadcast y bajo control de asignación de direcciones.

- Tampoco se mantiene control sobre el uso de recursos y servicios de la red a excepción del proxy de Petroecuador en el caso del uso del servicio de Internet.

- A esto también se suma el problema de estar usando una versión antigua de Antivirus, el cual proporciona un nivel bajo de protección ante las amenazas informáticas surgidas día a día.

- Tampoco se dispone de protección firewall en ninguno de los distritos poniendo en peligro toda la red LAN de cada refinería.

- No se tiene ningún control en la incorporación de equipos activos de red no administrables como switches de capa 2 y access point a la red LAN. A esto suma también la falta de aplicación de políticas de seguridad a nivel de los equipos que brindan servicio de conexión inalámbrica; siendo este uno de los puntos más vulnerables a nivel de la red LAN de cada distrito.

5.4.CUELLOS DE BOTELLA.

Dentro de la estructura de la red LAN y WAN de Petroindustrial a nivel nacional, se tiene bien claro que el servicio de interconexión de telecomunicaciones está formando parte de un convenio de cooperación entre filiales de Petroecuador; por lo que este servicio es prestado por Petrocomercial, dado que su infraestructura a nivel de enlaces de radio y microonda es muy robusta.

Esto involucra que Petroindustrial esté haciendo uso de un servicio que muchas veces se ve afectado por diversos factores como climáticos, deterioro de equipos, fallas del suministro eléctrico, e incluso fallas humanas, etc; ya que los enlaces o equipos de telecomunicaciones están instalados en diversos puntos la geografía nacional y que en muchas ocasiones son de difícil acceso.

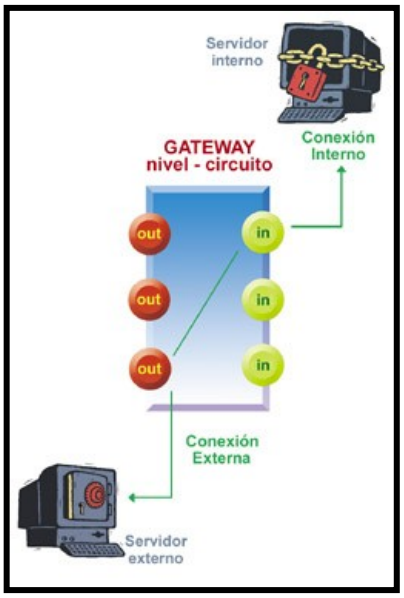


Fig: 5.4: Cuellos de Botella Red LAN Petroindustrial
FUENTE: Revista Red Escolar / Informática para todos / Firewalls.
"La importancia, sus políticas para la seguridad de una red":
http://redescolar.ilce.edu.mx/redescolar/Revista/10/articulos/08.html.2004-09-21

Haciendo referencia al aspecto detallado en los párrafos anteriores, podemos señalar algunos de los cuellos de botella que registra la red de Petroindustrial.

- Los enlaces de Telecomunicaciones entre Petroindustrial Matriz y Refinerías están sujetos al servicio prestado por los equipos de microonda y radio enlace que posee Petrocomercial a nivel nacional. Esto indica que por dichos enlaces no solo circule información de una sola red, lo que hace que el ancho de banda ofrecido sea compartido y por lo tanto eleve los tiempos de transmisión de información. Los enlaces con cada una de las refinerías en el mejor de los casos operan a 648 kbps que es el ancho de banda nominal.

- Otro de los cuellos de botella importante, es el indiscriminado uso de recursos de red, como el servicio de Internet, el cual tiene un ancho de banda específico y que por su uso irracional se ve copado casi en su totalidad la mayor parte del tiempo. Esto ocasiona molestias tanto por parte de los usuarios como lentitud en el resto de aplicaciones que fluyen a través de los enlaces de comunicaciones.

- No existe un adecuado control y monitoreo del tráfico de la red ni a nivel local LAN, ni a nivel nacional en la red WAN. Esto ocasiona que el consumo del ancho de banda sea excesivo y muchas de las veces sea ocupado por tráfico innecesario.

- La tecnología de encapsulamiento Frame Relay implementado en los ruteadores Motorola Vanguard hace que el proceso de transporte de la información, sea esta voz o datos se vea afectado por su proceso operacional ocasionando retardos excesivos en los tiempos de trasmisión.

- Dentro de la configuración de los equipos de enrutamiento administrados por Petrocomercial, se ha detectado que no se ha realizado en mucho tiempo una correcta depuración de las tablas de rutas y saltos, lo que ocasiona que se produzcan lazos entre dichos equipos ocasionando muchas veces la interrupción de los enlaces.

- La falta de aplicación de políticas de control que limiten el uso de recursos de red para favorecer al transporte de la información importante entre las diversas aplicaciones que sirven para el control y operatividad de las plantas de refinación, se convierte en otro de los cuellos de botella de la red de Petroindustrial.

- El uso de diversas marcas en los equipos activos de red también hace que los enlaces y configuraciones de la red se vean afectados, ocasionando retrasos y muchas de las veces cortes sorpresivos del servicio de enlace. Hay que sumarle a esto que el proceso de enviar datos y voz al mismo tiempo tiene sus desventajas si las configuraciones no son bien aplicadas dentro de cada equipo involucrado en los enlaces de telecomunicaciones.

- A más de los problemas citados anteriormente hay que recalcar uno muy importante, y que es la existencia de varios equipos Hub en puntos estratégicos de la red en las instalaciones de las refinerías. Estos equipos han sido instalados con el fin de satisfacer las necesidades del momento, pero que por su estructura de operación se vuelven una vulnerabilidad

- en la topología de la red. También son causa de inducir zonas de colisión y al no ser equipos activos de red administrables, no ofrecen la posibilidad de aplicar algún nivel de configuración adecuado y mucho menos pasar la configuración de subredes o vlan’s que eliminen las grandes zonas de broadcast.

- La existencia en las refinerías de enlaces de radio Punto a Punto y Multipunto para unir edificios distantes con tecnologías antiguas que no ayudan a la hora de mejorar la estructura y topología de la red, se convierten también en un cuello de botella que afecta el normal desempeño de la red LAN.

CAPITULO VI

ANÁLISIS DE CONFIGURACIONES EN EQUIPOS DE RED DE PETROINDUSTRIAL

6.1. Análisis de equipos de comunicaciones.
6.2. Configuraciones aplicadas dentro de la red.
6.3. Tecnologías soportadas por los equipos de red y telecomunicaciones.
6.4. Comprobación de configuraciones de los equipos de red

6. ANÁLISIS DE CONFIGURACIONES EN EQUIPOS DE RED DE PETROINDUSTRIAL

6.1.ANÁLISIS DE EQUIPOS DE COMUNICACIONES.

Al ser Petroindustrial una filial de Petroecuador, y por ende una de las empresas más productivas del país, hace que su estructura de funcionamiento a nivel nacional involucre en el ámbito tecnológico de la comunicación la incorporación de los últimos avances de la tecnología de redes y telecomunicaciones.

Pero esta carrera de actualización tecnológica también acarrea cierto tipo de problemas e inconvenientes, asociados con el tipo de equipos adquiridos, las versiones, capacidad y rendimiento, que son necesarias para el normal funcionamiento dentro de la estructura topológica de la red LAN y WAN de Petroindustrial.

Fig: 6.1: Equipos de Networking en Petroindustrial

FUENTE: Presentación Proyecto Optimización de Red de Datos – Petroindustrial 2007, Intro

Dado que estas características son determinantes a la hora de poner en operación un equipo activo de red o de telecomunicación, es necesario que se las tome muy en cuenta y se planifique con visión de crecimiento y previniendo necesidades futuras y eventos la adquisición de los mismos; a fin de prever que a futuras configuraciones y actualizaciones, los equipos presten las debidas facilidades tanto de software como de hardware para soportar dichos cambios, sin hacer necesario el reemplazo de un equipo; ya que esto ocasionaría tanto inversión de tiempo de trabajo como también de pérdidas por el obligatorio reemplazo de estos dispositivos.

6.2.CONFIGURACIONES APLICADAS DENTRO DE LA RED.

Las configuraciones aplicadas a nivel de los equipos de redes y telecomunicaciones en la matriz de Petroindustrial en Quito se detallan así:

Empezaremos por el equipo principal de core que es un Switch Router Cisco Catalyst 4507R; el mismo que tiene configurado toda la topología de VLAN's asociada a cada departamento ó unidad que conforman la estructura organizacional de Petroindustrial. Actualmente cada Vlan tiene un scope o rango de 32 direcciones IP, de las cuales solo se tiene disponibles 30, ya que la primera dirección y la última son direcciones de subred y de broadcast respectivamente.

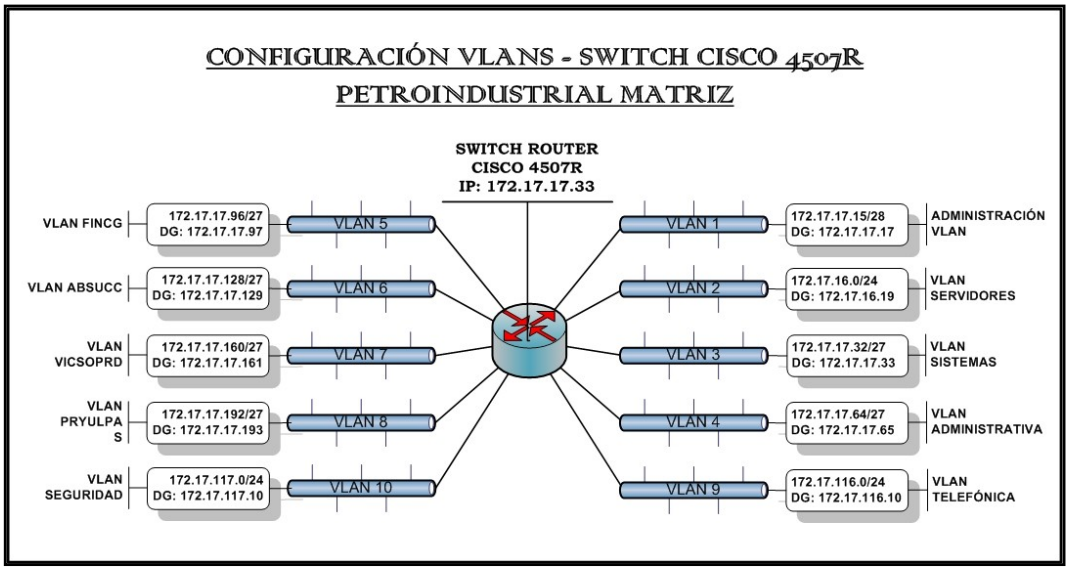


Fig: 6.2: Configuración de VLAN's Petroindustrial
FUENTE: Propio

Además también se ha especificado las direcciones de las redes y las subredes para el enrutamiento respectivo, ya que este equipo presta las facilidades de ser multilayer o multicapa, permitiendo manejar enrutamiento. De esta manera se encarga de realizar la respectiva conexión entre las diferentes subredes configuradas en él, así como también de proporcionar el respectivo enlace con el equipo principal de enrutamiento que tiene la unidad de Sistemas de Petroindustrial en la matriz de Quito.

Dentro del backbone de la red LAN de Petroindustrial en el edificio actual, se tiene ubicados cada 2 pisos equipos Switch del modelo Catalyst 3560 los mismos que son clientes VTP de equipo principal de core del centro de computo, que viene a ser el Cisco Catalyst 4507R. Estos equipos sólo se encargan de replicar la información topológica de la red configurada en el switch principal para poder distribuirla de acuerdo a la configuración y ubicación de las unidades y departamentos dentro del edificio.

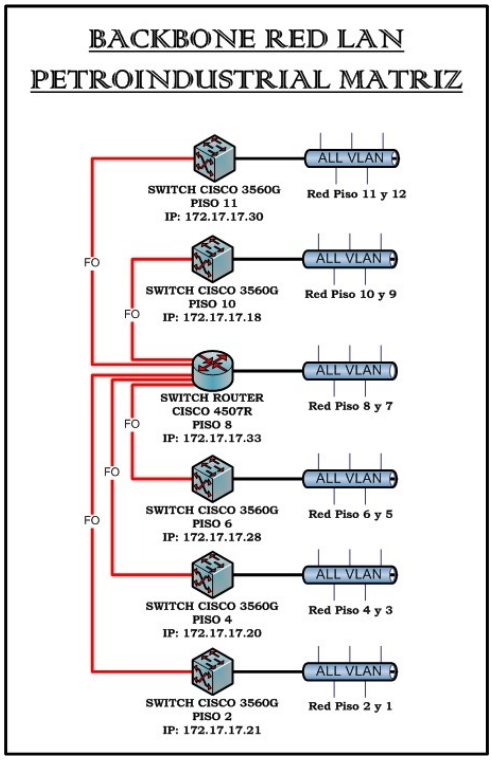


Fig: 6.3: Diagrama de Backbone Vertical Edificio Petroindustrial Matriz
FUENTE: Propio

Para el enrutamiento de las direcciones IP de la red LAN de Petroindustrial, tanto hacia las refinerías como hacia el servidor proxy de Internet en Petroecuador se tiene dentro del centro de computo un equipo Ruteador Motorola Vanguard, el mismo que tiene definido dentro de su tabla de rutas, las direcciones estáticas de las redes a las cuales se debe entregar los paquetes de las solicitudes generados en las subredes de Petroindustrial. Además, este equipo mantiene encendió el protocolo de enrutamiento Rip versión 2 que le facilita el descubrimiento de nuevas rutas para el envío de la información por distintos caminos facilitando así enrutamiento con los demás equipos de la red WAN de Petroindustrial a nivel nacional.

Fig: 6.4: Equipos Router Vanguard usados en Red LAN-WAN de Petroindustrial
FUENTE: TGS: Vanguard Router Solutions:
http://www.tgscorp.com/vanguard.php. Año 2006.

Las configuraciones aplicadas sobre los equipos de red y telecomunicaciones en las refinerías de Petroindustrial se detallan así:

Sobre las instalaciones de red y networking en las refinerías y dentro de su estructura topológica de administración, no se tiene implementado direccionamiento y segmentación a través de subredes y Vlan's, por lo que la zona principal de broadcast siempre es la Vlan nativa o Vlan 1 dentro de los equipos activos de red. Gran parte de los equipos de networking en las refinerías solo tienen configurados las direcciones IP de equipo con motivos administrativos, pero no se tiene realizado ningún trabajo de segmentación aplicado dentro de ellos.

La segmentación de la red en las refinerías se vuelve imperativa de implementar, más que nada por mantener y elevar el control, así como también, para permitir una mejor administración de los recursos de red que ofrecen los sistemas de redes dentro de las instalaciones físicas de estas dependencias; dado que al tener redes de menor tamaño permiten la existencia de dominios de broadcast más pequeños, aspecto importante para el diseño de red y la correcta utilización y optimización de recursos.

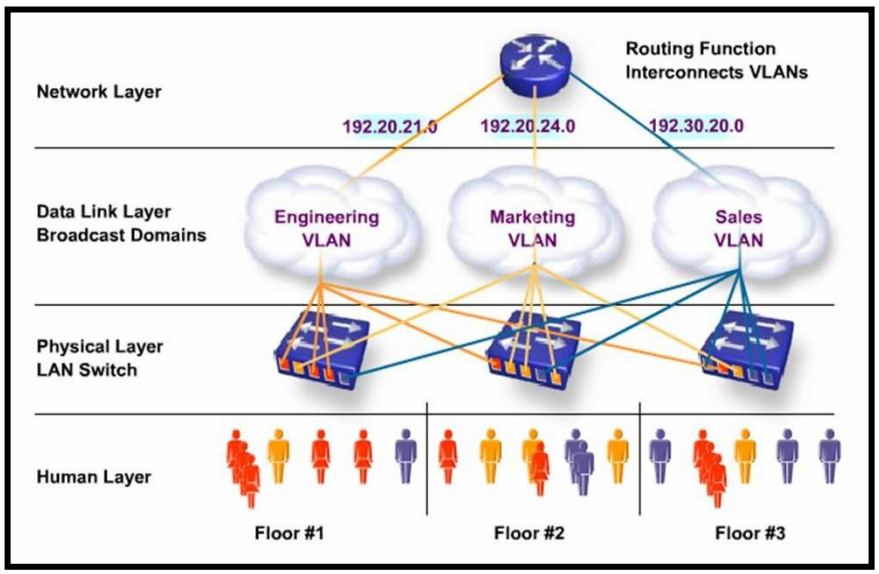


Fig: 6.5: Diagrama esquemático de subdivisión de redes LAN-WAN en VLANS.

FUENTE: Presentación Proyecto Optimización de Red de Datos – Petroindustrial 2007, Pág.: 21

Dentro de las configuraciones de los equipos de enrutamiento instalados en cada una de las refinerías, los cuales se encuentran bajo administración del Área de Telecomunicaciones de Petrocomercial por el convenio sostenido con Petroindustrial; se tiene establecido rutas estáticas de conexión para poder alcanzar los otros equipos de ruteo instalados dentro de la Red WAN de Petrocomercial, ya que se hace uso de la

infraestructura que ellos disponen para poder llegar a las diferentes instalaciones que dispone Petroindustrial en el país.

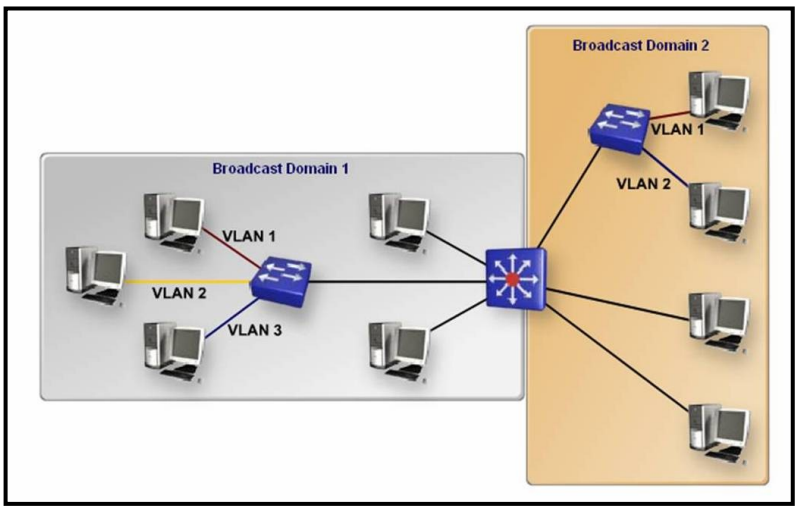


Fig: 6.6: Esquema de direccionamiento por dominios de broadcast

FUENTE: Presentación Proyecto Optimización de Red de Datos – Petroindustrial 2007, Pág.: 19

Además de las configuraciones para datos habilitadas dentro de estos equipos de enrutamiento que son de Marca Motorola Vanguard, instalados en las refinerías; se tiene también habilitados los canales de voz, para el envío y recepción extensiones telefónicas que permiten la comunicación ágil y oportuna entre las diferentes dependencias a nivel nacional.

6.3.TECNOLOGÍAS SOPORTADAS POR LOS EQUIPOS DE RED Y TELECOMUNICACIONES.

Para detallar las tecnologías soportadas por los equipos de red y telecomunicaciones, los separaremos según su aplicación específica; así:

Dentro de los equipos activos de la red LAN (swicthes) que pertenecen a la Matriz de Petroindustrial, por ser equipos relativamente nuevos y de capa 3, soportan todas las tecnologías necesitadas por las aplicaciones y servicios implementados dentro de la red. A más de esto, están completamente preparados para soportar cambios tecnológicos como la migración a full telefonía IP, balanceo de carga y alta disponibilidad de servicio, ya que ofrecen la posibilidad de incorporar redundancia para su operación. Dentro de los equipos de red LAN se detallan a continuación los siguientes:

1. Switch Cisco Catalyst 4507R de 144 puertos RJ45 10/100/1000 Mbps, más 8 puertos up-link de fibra óptica; con IOS (Sistema Operativo) en versión 12.1(19)EW1., que funciona como switch de core o principal. Es en este equipo donde se tiene implementada la configuración principal de Vlan's y servicios y de donde se reparte a los demás equipos del backbone de red.

2. Switch Cisco Catalyst 3560G de 48 puertos 10/100/1000 Mbps, más 4 puertos up-link de fibra óptica, con IOS (Sistema Operativo) en versión 12.2(25)SEB4, que complementan el backbone vertical del edificio.

3. Switch Cisco Catalyst 2970G de 24 puertos 10/100/1000 Mbps con IOS (Sistema Operativo) en versión 12.2(25)SEB4. Este equipo está cumpliendo la función de convertidor de medio entre fibra óptica y cobre; y además permite la interconexión con el equipo principal de enrutamiento Motorola Vanguard 6455.

A nivel de las refinerías y dentro de los equipos de red LAN, también se especifica que los equipos soportan todos los servicios y tecnologías implementados dentro de su red lógica; pero también hay que hacer hincapié en los equipos que se encuentran fuera del servicio de desarrollo y mantenimiento de CISCO SYSTEMS; ya que en las instalaciones de físicas de las refinerías si se encuentra equipos como los ruteadores Cisco 1601R los cuales por su versión de IOS ó sistema operativo no permiten la implementación de VLAN's y son un cuello de botella para el crecimiento tecnológico de la infraestructura de red.

A nivel de los equipos de enrutamiento dentro de la red WAN de Petroindustrial, es decir los equipos Motorola Vanguard se especifica que están en las mejores condiciones de operación y que además por estar funcionando con la última versión de sistema operativo (V.6.4), soportan tecnologías de enrutamiento de alta velocidad y también tienen un gran rendimiento a la hora de manejar el encapsulamiento de voz. Estos equipos permiten incorporar tarjetas de conexión FXS y FXO para el envío de extensiones ó líneas telefónicas a través de la red WAN de Petroindustrial. Entre las tecnologías soportadas por los equipos Vanguard están: ATM, Frame Relay, ISDN.

6.4.COMPROBACIÓN DE CONFIGURACIONES DE LOS EQUIPOS DE RED.

Las configuraciones aplicadas en los equipos de red para la operación adecuada de las mismas, cumplen con las normas especificadas por el fabricante de los equipos, y se mantiene un riguroso control de cambios y backup en caso de presentar algún

inconveniente. Además previo a la realización de un cambio de configuración, se hace una planificación de trabajo, documentación y contingencia a fin de que si se presenta algún problema, este pueda ser superado inmediatamente. Y por su puesto cada cambio es comunicado con anticipación al personal de sistemas a fin de prestar la respectiva colaboración en caso de inconvenientes.

Como se especificó antes, el concepto principal manejado dentro de la red LAN de cada distrito de Petroindustrial es el manejo de VLAN's para establecer un mejor control y empezar a manejar seguridad dentro del domino de broadcast de la red. Pero es en la Matriz donde únicamente se maneja este tipo de configuración de VLAN´s ya que se tiene implementado la subdivisión de una subred por cada unidad o departamento de la estructura organizacional de la empresa. En los demás distritos únicamente se maneja la Vlan default o nativa (N° 1), y es donde se encuentran todos los equipos, inclusive los servidores de red. Esto ocasiona que se genere un gran dominio de broadcast provocando retardos y bajo rendimiento de los servicios dentro de la red.

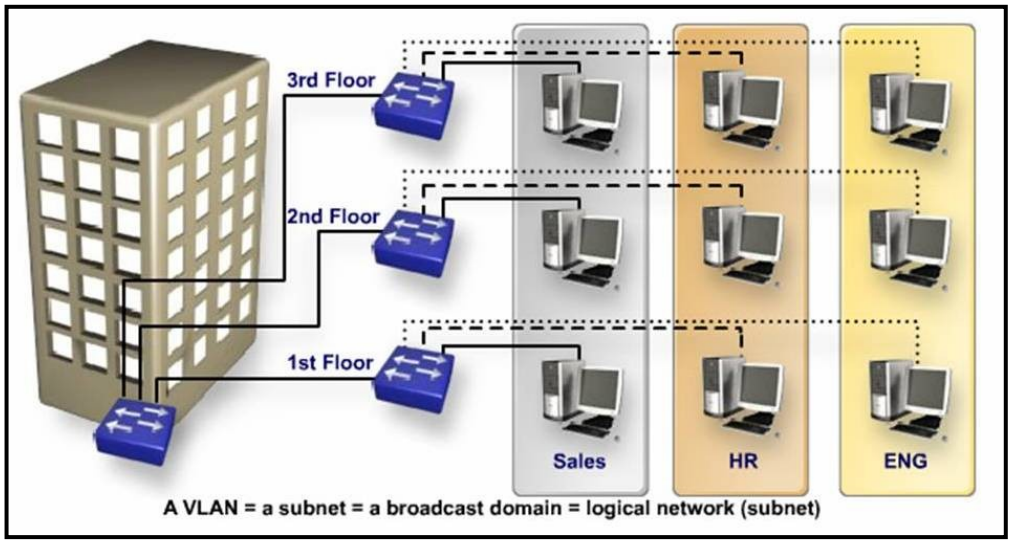


Fig: 6.7: Esquema de subdivisión en VLAN's de una red por secciones o departamentos.

FUENTE: Presentación Proyecto Optimización de Red de Datos – Petroindustrial 2007, Pág. 18

Se puede decir que dentro de las configuraciones aplicadas en los equipos de networking, la red LAN de Petroindustrial Matriz, sirve de prototipo para las demás refinerías, dado que se está planificando un proyecto de reestructuración del esquema de direccionamiento IP de red aplicando Vlan's de acuerdo con la constitución organizacional de cada refinería. Luego de realizado y terminado este proyecto, se viene la planificación e implementación de procedimientos de seguridad, administración, optimización y monitoreo de recursos de la red cada distrito a fin de elevar el performace y rendimiento de toda la infraestructura de networking que tiene montada Petroindustrial en todas sus instalaciones de operación.

CAPITULO VII

ADMINISTRACIÓN DE REDES CON CISCOWORKS

7.1. Introducción a CiscoWorks.

7.2. Características de la herramienta.

7.3. Módulos de trabajo y administración de red.

7.4. Configuraciones para administrar y monitorear una red con Cisco Works

7. ADMINISTRACIÓN DE REDES CON CISCOWORKS

7.1.INTRODUCCIÓN A CISCOWORKS.

CiscoWorks es una herramienta de Software propia de la Marca CISCO SYSTEM dedicada al control, manejo, administración, actualización y monitoreo de los equipos Switch y Ruteadores Cisco. Al ser una herramienta muy poderosa y propia de la marca, permite al usuario/administrador, manipular y mantener en orden los equipos durante su funcionamiento, así como realizar múltiples tareas relacionadas con la administración y uso de recursos de manera óptima, dentro de una red LAN o WAN.

La herramienta está desarrollada en lenguaje de programación JAVA y con una Base de Datos SYSBASE, su interfaz de trabajo es amigable (página web), y ofrece mucha versatilidad a la hora de realizar tareas de administración o configuración de los equipos CISCO. CiscoWorks es una familia de productos para la administración de redes empresariales que se ha empaquetado o aliado, enfocado en arquitecturas o funciones de red específicas.[29]

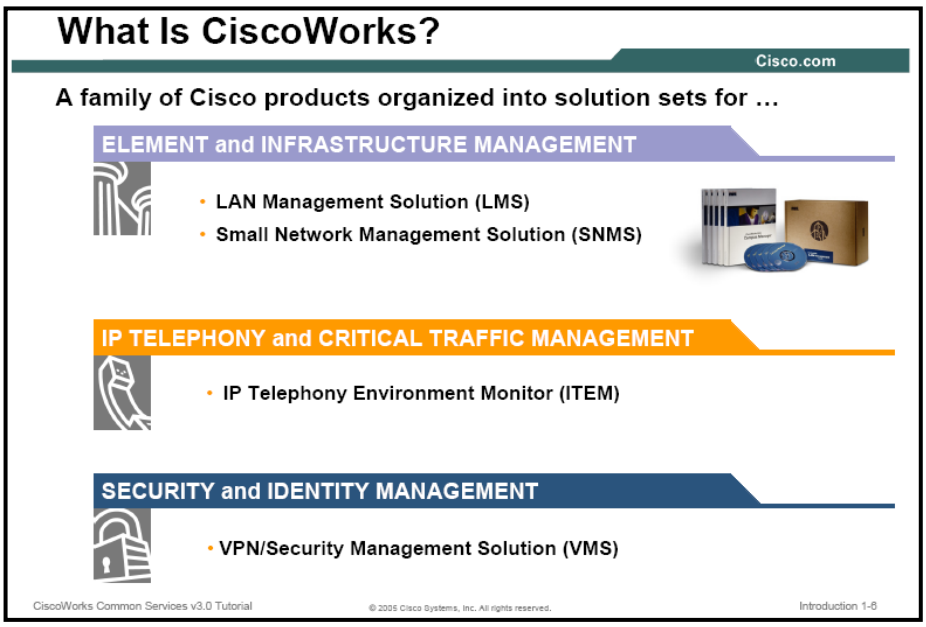


Fig: 7.1: Estructura y Familia de Productos de CiscoWorks.

FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc. 2005, Pág.: 1-6

CiscoWorks tiene una nueva arquitectura que ha heredado flexibilidad, escalabilidad, y extensibilidad. Los productos dentro de la familia CiscoWorks representan un avance

[29] CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005

significativo hacia "Administración de Intranets" basados en WEB y eso, permite integración, accesibilidad y despliegue. CiscoWorks usa los estándares de Internet de las aplicaciones, permitiendo la integración con populares NMSs (Network Management System) socios de CISCO.

CiscoWorks está construido sobre nuevos estándares de Internet, pero confía en la inteligencia construida en los IOS de Cisco, Catalyst software, y en los agentes o servicios que corren sobre los dispositivos Cisco. Al poner inteligencia en la red de una empresa, permite que esta sea escalable y manejable.

CiscoWorks son una familia de herramientas de administración de red que permiten que el administrador acceda fácilmente y maneje las capacidades avanzadas de la arquitectura de Cisco para la voz, video y la integración de los datos (AVVID). Las herramientas proveen innovadores maneras de administrar centralizadamente las características críticas de la red como la disponibilidad, la capacidad de respuesta, la resistencia, y la seguridad de una manera consecuente.

La familia de productos CiscoWorks ayuda a reducir el tiempo la incertidumbre relacionada con la introducción de nuevos servicios como la voz, redes inalámbricas y administración. Las herramientas han sido enfocadas en soluciones complementarias de CiscoWorks de punta con punta que son diseñadas para manejar los dispositivos eficientemente, las configuraciones, usuarios, y servicios en una red. La naturaleza modular de productos de CiscoWorks, permite que el administrador de la red seleccione herramientas que necesita de un largo rango de soluciones para la clase de empresa que necesite.

7.2.CARACTERÍSTICAS DE LA HERRAMIENTA.

Los productos de Cisco Systems, en este caso CiscoWorks está basado en la arquitectura Cliente/Servidor, lo que permite a múltiples clientes basados en Web acceder al servidor de administración en la Red. Mientras que el número de los dispositivos de la red aumenta, los servidores o los puntos adicionales se pueden agregar fácilmente con poco impacto en el uso del browser del cliente, haciéndolo muy escalable.

El servidor CiscoWorks proporciona funciones comunes tales como el motor de la base de datos, la ayuda en línea, la seguridad, conexión o login, lanzar aplicaciones, trabajos o procesos de administración, y el servidor web. Esto proporciona un interfaz común para todos los productos CiscoWorks.

Los productos de CiscoWorks interactúan con los dispositivos administrables de Cisco, colectando la información. Los productos usan protocolos comunes como Simple Network Management Protocol (SNMP), Telnet, Trivial File Transfer Protocol (TFTP), y Remote Copy Protocol (RCP) para acceder a los dispositivos y extraer la información necesaria; pero en especial CiscoWorks opera utilizando el protocolo propietario de Cisco Systems CDP – Cisco Discovery Protocol, el cual debe estar habilitado en cada uno de los dispositivos administrables para que la información de cada equipo pueda ser accedida por parte de CiscoWorks.

CiscoWorks Server puede también conectarse hacia Cisco Connection Online (CCO), sitio Web propio de Cisco Systems que ofrece Recursos del Sistema basado en Web para realzar funciones tales como obtención de actualizaciones del producto, descarga de IOS (Sistemas Operativos), documentación y de asistencia técnica en caso de ser necesaria.

En el siguiente gráfico se detalla la arquitectura operacional y funcional de CiscoWorks.

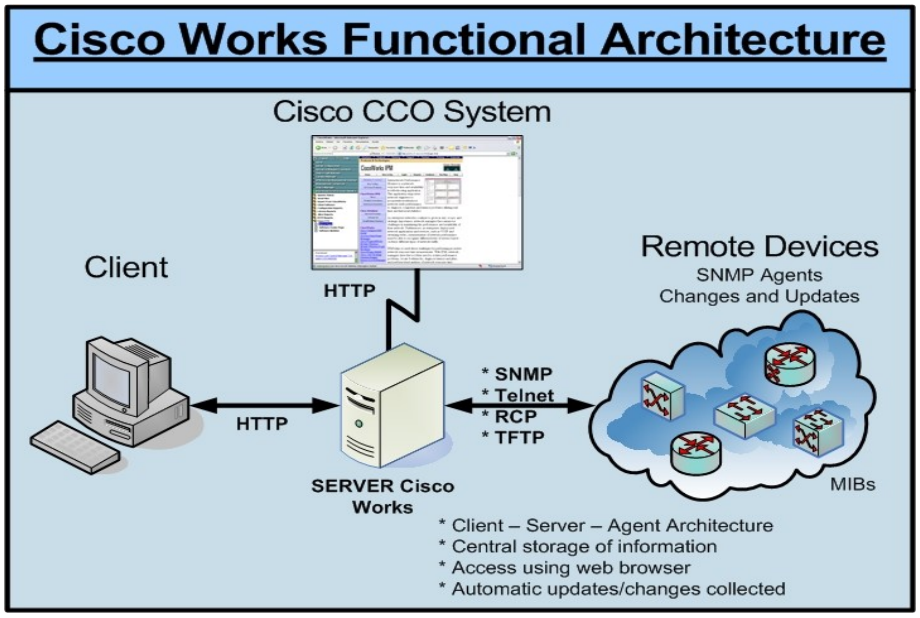


Fig: 7.2: Diagrama de Arquitectura Operacional de CiscoWorks

FUENTE: Propio

7.3.MÓDULOS DE TRABAJO Y ADMINISTRACIÓN DE RED.

CiscoWorks es una suite de aplicaciones consistente en productos para administración de red apuntadas hacia las redes empresariales. Los productos CiscoWorks soportan día a día las tareas de administración de red y sus crecimientos

futuros. También contienen un arsenal grande de funciones para localización de problemas (diagnóstico) y mantenimiento.

La familia de productos CiscoWorks para administración de redes empresariales se ha empaquetado o "se ha aliado" enfocándose en arquitecturas y funciones específicas de red. No muchos de los clientes tienen que elegir entre aplicaciones individuales para satisfacer sus necesidades de administración de red. Simplemente se determina si se encuentra en la necesidad de Administrar un campo LAN, Administración WAN, Administración a Nivel de Servicio, o Soluciones de Administración de Seguridad VPN.

La Familia CiscoWorks incluye los siguientes administradores de Red.[30]:

1. LAN Management Solution (LMS)
2. Routed WAN Management Solution (RWAN)
3. Service Management Solution (SMS)
4. VPN/Security Management Solution (VMS)
5. Campus Bundle for AK/HP-UX

LAN Management Solution; comprende aplicaciones en WEB para configuración, administración, monitoreo y solución de problemas de una red de campo, LAN.

Routed WAN Management Solution; comprende aplicaciones de administración empresarial para configurar administrar, monitorear y solucionar problemas de ruteo de una red de área amplia, WAN.

La solución Routed WAN Management Solution incrementa la visibilidad del comportamiento de una red y reduce la complejidad en el manejo del ruteo de una red de área amplia WAN.

Service Management Solution (SMS); provee aplicaciones para implementar Acuerdos de Nivel de Servicio (SLAs). SLAs responde las necesidades de administración de la empresa, para tener la seguridad de que los servicios y aplicaciones estarán disponibles por parte de los proveedores IT e ISPs.

VPN/Security Management Solution (VMS); provee aplicaciones para monitoreo y solución de problemas a nivel de Redes Privadas Virtuales (VPNs) y además aplicaciones para configurar y monitorear la seguridad de los Firewall.

[30] Implementing CiscoWorks LMS Vol.1 versión 2.5 CWENT v2.5. Año 2005.

Campus Bundle for AIX/HP-UX; provee aplicaciones para configuración, administración, monitoreo y solución de problemas para redes de campo LANs. Las aplicaciones proporcionadas en este paquete son un subconjunto de los productos CiscoWorks. No todas las características están disponibles para las plataformas ADC y HP-UX, y los lanzamientos que están disponibles no son la última versión.

7.3.1. **LAN Management Solution.**[30]

Para este estudio nos enfocaremos en la principal herramienta de servicio y administración de red que posee CiscoWorks que es LMS - LAN Management Solution.

El LMS de CiscoWorks es una solución que contiene algunas de las más comunes aplicaciones usada para administrar dispositivos de red Cisco. Usando estas aplicaciones, los directores de la red pueden proveer configuraciones comprensivas, administración de fallas, y el rendimiento de redes basadas en Cisco. La Web de CiscoWorks suministra puntos de lanzamiento para aplicaciones de CiscoWorks y las funciones más importantes instaladas sobre el servidor de CiscoWorks local o en los servidores remotos.

LMS está conformada de las siguientes herramientas descritas a continuación.

- Common Services
- Cisco View
- Resource Manager Essentials
- Campus Manager
- Device Fault Manager
- Internetwork Performance Monitor
- Device Center.

7.3.1.1. **Common Services.**[29]

Common Services es un conjunto de servicios de administración compartido por más de una aplicación de administración, en sí, la mayoría de los productos de CiscoWorks dependen de él. Common Services le permite manejar los roles de usuario y privilegios, manejar el control de acceso a las aplicaciones, tanto como a las características especiales

[30] Implementing CiscoWorks LMS Vol.1 versión 2.5 CWENT v2.5. Año 2005.
[29] CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005

dentro de las aplicaciones. Los roles y privilegios son controlados por los servicios de autentificación y autorización incorporados, o a través de un servidor de Control de Acceso Externo (ACS).

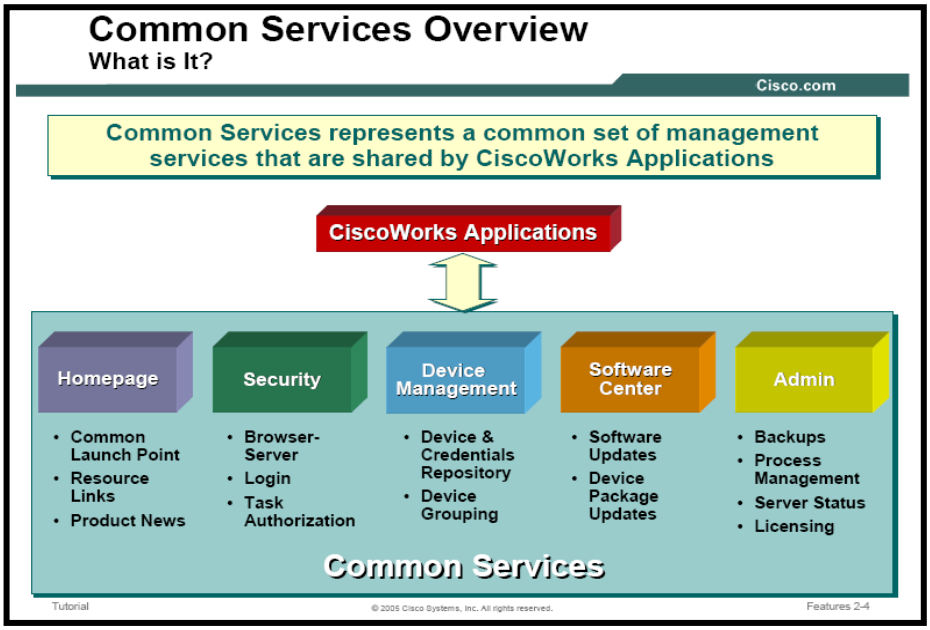


Fig: 7.3: Diagrama Estructural de Operación de Common Services – CiscoWorks

FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005, Pág.: 2-4

El servidor de Common Services de CiscoWorks es diseñado como una infraestructura de tres pisos compuesta de estos servicios:

Runtime services: que comprende la Página Web, Procesos de administración, seguridad y motor de ayuda

System services: comprende el motor de base de datos y utilidades, tanto como servicios de distribución de eventos y administrador de trabajos.

Core services: Usado para el manejo de las aplicaciones centrales.

7.3.1.2. Cisco View.[31]

CiscoView es una aplicación fácil de usar y gráfica, que permite que el usuario configure y monitoree un dispositivo de Cisco. Viene como paquete auto-instalado con el Common Services. Los asistentes de CiscoView, permiten una visualización física de un dispositivo de Cisco, los identifica por color y permite describir el estado de puerto, lo que permite que usted comprenda la información esencial rápidamente. Las características de CiscoView, permiten ver el estado dinámico, el monitoreo del dispositivo, y la información de configuración exhaustiva para productos de internet working de Cisco como ruteadores, switches y productos de acceso.

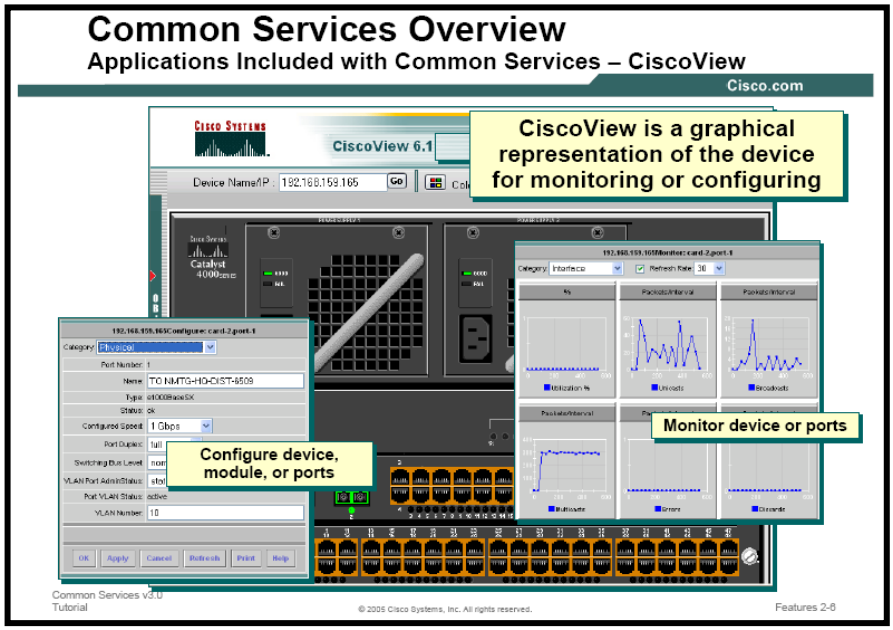


Fig: 7.4: Diagrama Operacional de CiscoView de CiscoWorks

FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005, Pág: 2-6

Las características de CiscoView permiten que usted haga lo siguiente:

- Ver una representación gráfica del dispositivo, incluyendo el estado componente como interfaz, tarjeta, suministro de energía, y estado de LED.
- Configuración de parámetros para dispositivos, tarjetas, e interfaces.
- Monitoreo estadístico en tiempo real para interfaces, la utilización de recurso, y el rendimiento de dispositivo.
- Fijar las preferencias del usuario.
- Llevar a cabo operaciones específicas en los dispositivos

[31] CiscoView v6.1 Tutorial Cisco Systems, Inc 2005

- Dirigir un grupo de dispositivos.

7.3.1.3. Resource Manager Essentials.[32]

RME se concentra principalmente en el aspecto administrativo de configuración de la red. Incluye muchas características especiales que simplifican las tareas de dirección de configuración, como: llevar a cabo actualizaciones del software o cambiar archivos de configuración sobre múltiples dispositivos. RME también incluye las características de administración de fallas a través de filtrar los mensajes de syslog. RME consta de estas funciones muy importantes, tanto como algunas características adicionales que usted puede usar para administrar dispositivos de Cisco.

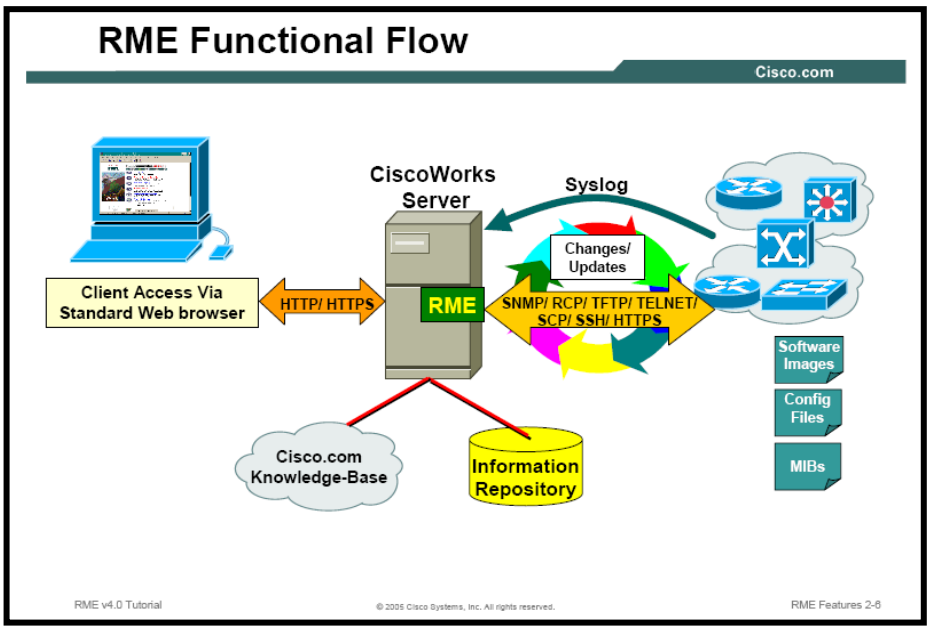


Fig: 7.5: Diagrama Operacional de Resource Manager Essentials

FUENTE: RME v4.0 Tutorial Cisco Systems, Inc 2005, Pág: 2-6

Inventory Management: Todas funciones de RME están basadas las credenciales de los dispositivos y las cuales son almacenadas en un depósito llamado DCR. Las credenciales guardan información detallada sobre cada dispositivo administrado por el servidor de RME. Inventory Management exhibe esta información a través de un juego extensivo de reportes

[32] Resource Manager Essentials RME v4.0 Tutorial Cisco Systems, Inc 2005

Configuration Management: La función del administrador de configuraciones, es almacenar la versión actual y previas versiones de los archivos de configuración para los dispositivos Cisco soportados y manejados por el RME Inventory. El número de versiones previas almacenadas es configurable. Si suceden cambios en la versión de los archivos, estos cambios se relejan inmediatamente en los archivos almacenados. Dos funciones adicionales están disponibles para editar los archivos de configuración NetConfig y Config Editor.

NetConfig: Permite almacenar un conjunto de comandos y ejecutarlos al mismo tiempo en muchos más dispositivos. Config Editor, permite la edición y descarga individual de archivos de configuración hacia los dispositivos a través del interfaz de línea de comandos.

Software Management: La función de esta aplicación es guardar una o más copias de las imágenes de software que funcionan en los dispositivos Cisco soportados de la red. También puede ser utilizada para actualizar las imágenes en los dispositivos de uno en uno o por grupos al mismo tiempo, permitiendo en caso de errores retroceder a la versión que corría correctamente sin problemas

Syslog Analysis: Su función es almacenar los mensajes de syslog de cualquier dispositivo configurado para enviar los mensajes de syslog al servidor de RME. Usted puede personalizarlo filtrando los mensajes, o ejecutar a series de comandos automáticamente si un mensaje específico es detectado. Por ejemplo, usted puede enviar un correo electrónico al administrador de la red si un error de nivel crítico ocurre sobre un dispositivo de la red importante. Syslog permite generar informes rápidamente.

Change Audit Services: La función de servicios de auditoría de cambios, permite que usted siga los cambios hechos a las funciones varias dentro de la red. Almacenan la información detallada sobre cualquier cambio que se han hecho a las imágenes existentes de software, y archivos de configuración. Esta información permite que el usuario esté al día con los cambios en caso de que haya problemas.

Audit Trail: es similar a la anterior función, pero en lugar de registrar los cambios para dispositivos, Audit. Trail está al día e informa sobre los cambios que el administrador hace sobre el servidor de RME.

7.3.1.4. Campus Manager.[33]

Campus Manager se enfoca principalmente sobre la dirección de configuración, tanto la conectividad física y lógica de dispositivos, como estaciones finales. Consta de estas tres herramientas distintas que pueden ser usadas para manejar y monitorear equipos de Capa 2 y Capa 3 de Cisco en la red.

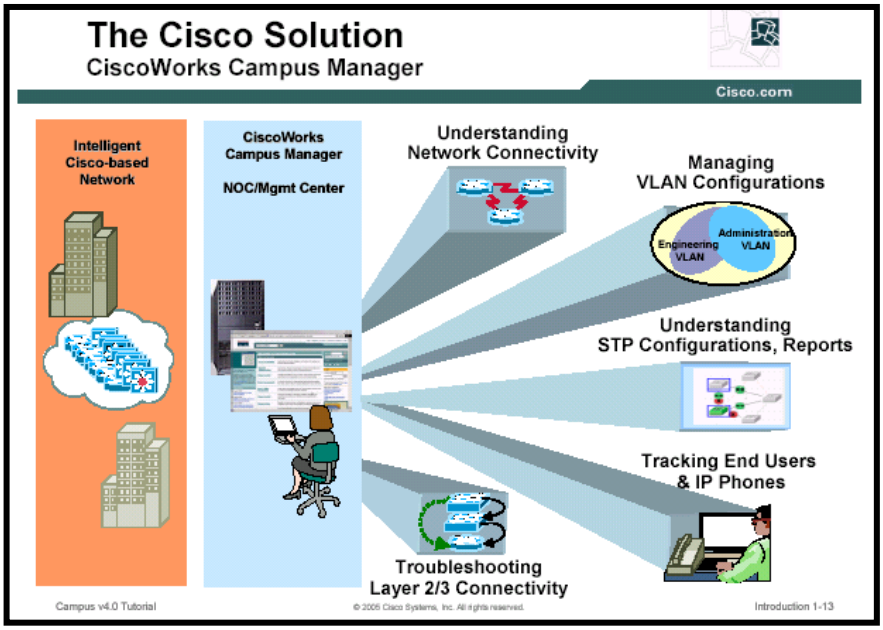


Fig: 7.6: Diagrama Estructural de Operación de Campus Manager de CiscoWorks

FUENTE: Campus v4.0 Tutorial Cisco Systems, Inc 2005, Pág: 1-13

Topology Services: Permite identificar todos los equipos soportados y descubiertos en un mapa muy ilustrativo, además puede agrupar los dispositivos por dominios VTP o según el administrador los quiera agrupar. Presenta también las discrepancias encontradas dentro de la topología de red de los equipos descubiertos.

Path Analysis: Permite realizar un trazado de ruta entre un origen y un destino, permitiendo ver el camino o ruta que siguen los paquetes por entre los equipos de capa 2 y 3 de una red. Detalla también la información de cada salto que dan los paquetes de información.

User Tracking: Es una herramienta que permite el manejo de los dispositivos de red finales, es decir los host o estaciones conectadas a los equipos Cisco. Puede identificar

[33] Campus v4.0 Tutorial Cisco Systems, Inc 2005

información detallada como MAC Address, IP Address, host name, DNS, puerto asignado y VLAN correspondiente.

7.3.1.5. Device Fault Manager.[34]

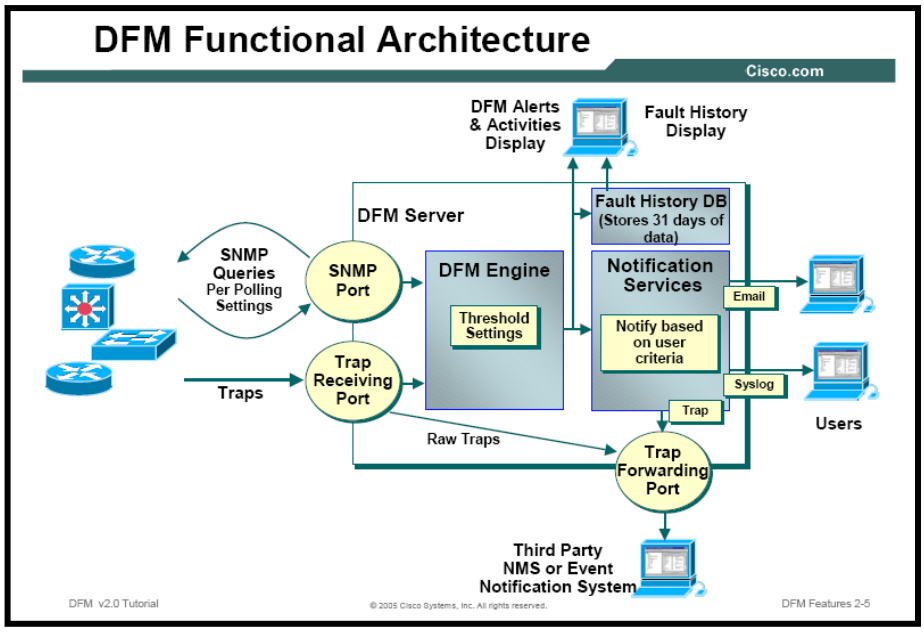


Fig: 7.7: Diagrama Operacional de Device Fault Manager de CiscoWorks

FUENTE: DFM v2.0 Tutorial Cisco Systems, Inc 2005, Pág.: 2-5

El Administrador de Fallas de red es vital para el éxito de una compañía. Tradicionalmente, los administradores de fallas sólo determinaban si un dispositivo estaba arriba o fuera de servicio. Con la complejidad de los equipos y la infraestructura de la red de hoy, un dispositivo puede estar ARRIBA, pero funcionar mal, resultando en la degradación de rendimiento de la red. La mayoría de los administradores de fallas, permiten que usted sondee variables de MIB específicas de forma selectiva para determinar la salud en conjunto de un dispositivo. Sin embargo, este sondeo selecto, requiere muchos conocimientos de determinar qué constituir una estratagema próspera, y qué variables de MIB sondear para determinar su salud.

DFM de Cisco aborda estos asuntos directamente. DFM escucha los mensajes de SNMP y tiene la inteligencia para sondear variables de MIB predeterminadas para la mayoría de los dispositivos de Cisco. DFM correlaciona los eventos múltiples

[34] Device Fault Manager DFM v2.0 Tutorial Cisco Systems, Inc 2005

"entonces/luego" juntos y los exhibe como los alertas para determinar la salud de un dispositivo sin la intervención del usuario.

7.3.1.6. Internetwork Performance Monitor.[35]

El crecimiento continuo de las redes de hoy crea nuevos desafíos para el administrador de la red con el fin de mantener rendimiento y disponibilidad. Demasiado a menudo, el usuario final informa sobre el rendimiento de la red y la disponibilidad es emitida después de que las aplicaciones más actúan normalmente. La típica descripción del síntoma es "La red está fuera de servicio", o "La red es lenta." Los directores de la red necesitan una manera más eficaz de descubrir el retraso de la red antes de que afecte al usuario final. A menudo usted necesitará que los datos serenos prueben que no es la red.

IPM suministra al administrador de la red la habilidad de medir los tiempos de respuesta de la red, determinar la disponibilidad y analizar dibujos de tiempos de respuesta de punta con punta también como de enrutador a enrutador ó de salto por salto. IPM también advierte al administrador de la red de las demora largas usando tramas de SNMP y los eventos que permiten que el administrador de la red solucione los asuntos de rendimiento potenciales proactivamente antes de que afecten al usuario final. Para medir la información de los tiempos de respuesta precisamente, IPM mide el rendimiento del tráfico de aplicación de la empresa directamente. Usar solamente ping para medir los problemas tiempos de respuesta no puede ser suficiente. Medir la demora de los datos de voz y los otros protocolos de capa superiores, como el protocolo TCP, el protocolo de datagrama (UDP), DNS, y protocolo de configuración del DHCP, puede proveer la información importante para optimizar la red.

7.3.1.7. Device Center.

Device Center suministra una vista dispositivo para aplicaciones CiscoWorks, permitiendo emitir informes sobre el comportamiento de un dispositivo específico, y así puede hacer actuar la demás herramienta para la correcta reparación técnica en caso de fallas.

[35] Internetwork Performance Monitor IPM v2.6 Tutorial Cisco Systems, Inc 2005

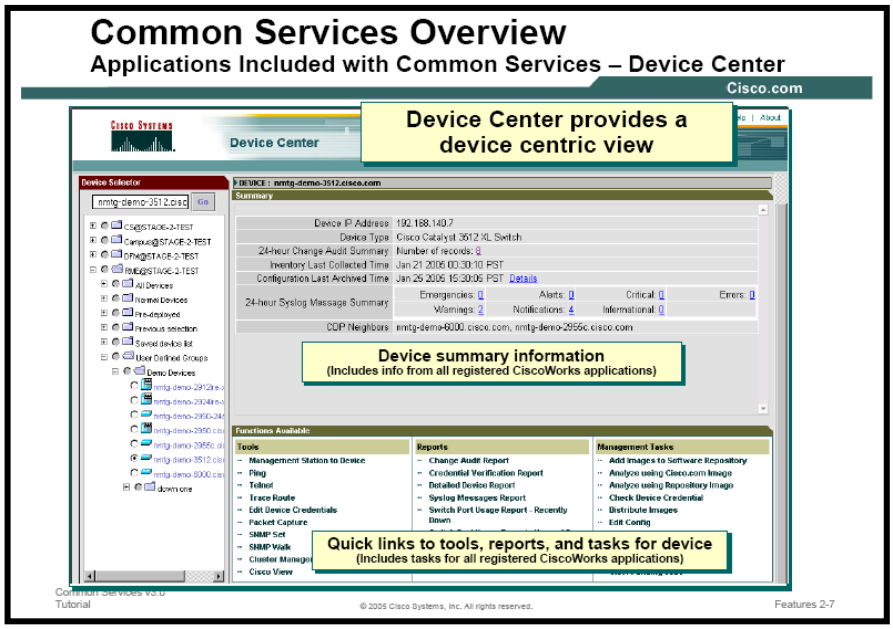


Fig: 7.8: Diagrama de Operación de Device Center de CiscoWorks
FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005, Pág: 2-7

Dentro de las actividades que se puede realizar en Device Center están el cambiar los atributos de dispositivo, actualizar el inventario, realizar Telnet, y mucho más dependiendo de las aplicaciones que son instaladas sobre el servidor Common Services local.

7.4.CONFIGURACIONES PARA ADMINISTRAR Y MONITOREAR UNA RED CON CISCOWORKS.

Dentro de las configuraciones específicas que se deben tener como base para administrar y monitorear una red LAN y todos sus equipos activos dentro de la misma al utilizar CiscoWorks se tiene las siguientes que describiremos a continuación.

Ya que este sistema de administración es propietario de una marca, que en este caso es Cisco Systems, hay que recordar que como fabricante, este busca la manera de optimizar el desempeño de sus equipos y herramientas, haciendo uso de sus propios protocolos y sistemas desarrollados por ellos mismos; pero a su vez se ven obligados a utilizar los diversos estándares y protocolos que existen en el mercado para poder competir y mantener su nivel frente a sus competidores.

Para el caso de CiscoWorks se deben tener las siguientes configuraciones para hacer un equipo alcanzable, administrable y monitoreable a la vez:

- Se debe tener habilitado el protocolo CDP – Cisco Discovery Protocol, propietario de Cisco que sirve para, permitir la comunicación entre sus equipos.

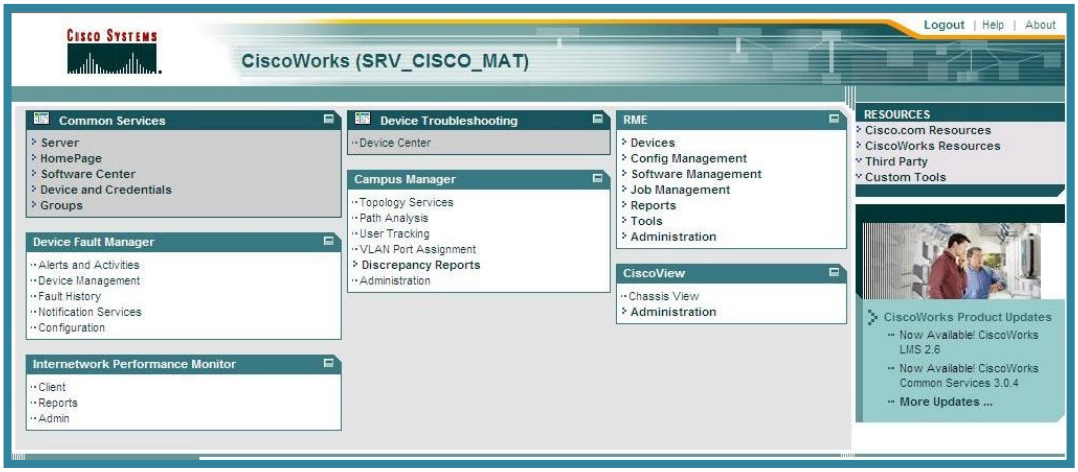
- Deben los equipos a ser administrados por esta herramienta tener configurada una dirección IP de administración con el objetivo de volver alcanzable al equipo desde las herramientas que incorpora este paquete. Con esta configuración dentro de los equipos se pueden habilitar varias opciones y agentes, que serán de mucha utilidad cuando las herramientas de este paquete de administración intenten realizar alguna acción sobre el equipo o la configuración que esté operando en el mismo

- Se debe tener habilitado y configurado SNMP – Simple Network Management Protocol dentro de los equipos; así como también las comunidades de lectura y escritura fijadas de acuerdo a los criterios de administración. De esta forma se podrá administrar y manejar un equipo mediante un protocolo estándar del mercado de networking, y al tener identificadas y configuradas las comunidades SNMP de administración harán posible la ejecución de todas las acciones necesarias en el caso de solucionar fallas o atender a un equipo.

- Se debe confirmar que el agente SNMP de cada equipo este corriendo, enviando y recibiendo la información solicitada por la herramienta de administración; ya que en algunos casos y dependiendo del tipo de equipo a ser administrado puede ser que el agente ejecutor del protocolo SNMP no se active al inicio; o en algunos casos si las comunicaciones pasan por un equipo firewall; este deniegue el paso de los paquetes enviados por SNMP. Para lo que se tendrá que habilitar el permiso necesario para, permitir el uso de este protocolo.

- Debe fijarse en la configuración de administración de la herramienta las comunidades de lectura y escritura especificadas para SNMP en los equipos de forma que, permita la interacción de los equipos de networking con los agentes de recolección de información de dispositivos Cisco. Así la herramienta dispondrá de toda la potencialidad que le brinda este protocolo para poder operar correctamente un equipo activo de red.

CAPITULO VIII



DISEÑO, CONFIGURACIÓN E IMPLEMENTACIÓN DE LA HERRAMIENTA DE MONITOREO DE RED CISCOWORKS Y REGLAMENTACIÓN DEL USO DE SERVICIOS

8.1. Estudio y diseño de reglamentos para administración de red.

8.2. Aplicación de los reglamentos para administración con CiscoWorks.

8.3. Reglamentación de uso de servicios y recursos de red utilizando CiscoWorks.

8.4. Análisis de servicios y recursos a monitorear dentro de la red.

8.5. Implementación de monitoreo sobre la red LAN y WAN de Petroindustrial con CiscoWorks.

8.6. Verificación de resultados de administración de red mediante monitoreo de recursos en la red de Petroindustrial.

8. DISEÑO, CONFIGURACIÓN E IMPLEMENTACIÓN DE LA HERRAMIENTA DE MONITOREO DE RED CISCOWORKS 2000 Y REGLAMENTACIÓN DEL USO DE SERVICIOS.

La administración de redes puede definir en términos de metas las esperanzas de la compañía de implementar una estrategia para realizar una administración competitiva de la red, más aún cuando actualmente los servicios y los métodos de proveerlos son transparentes para los usuarios. Para asegurarse de que estas necesidades estén resueltas los administradores en ingenieros de red necesitan una efectiva forma de administrar las complejidades que presenta una red, proveer máxima eficiencia y minimizar el tiempo de caídas preparándose así para la recuperación ante desastres.

Para lograr obtener un método de administración de red eficiente hay que basarse en modelos establecidos, enfocándose siempre en las particularidades que tiene cada empresa, en este caso Petroindustrial.

- **Definición del Modelo FCAPS.**[30]

Es así que analizaremos el modelo FCAPS para administración de redes estandarizado por la ISO. Definido inicialmente por ITU-T con especificaciones de FCAPS para las redes de la telecomunicación; pero los mismos conceptos se pueden aplicar a las redes de datos.

ISO define 5 áreas funcionales para la administración de redes.

1. Fault management
2. Configuration management
3. Accounting management
4. Performance management
5. Security management

[30] Implementing CiscoWorks LMS Vol.1 versión 2.5 CWENT v2.5

Fig: 8.1: Definición del Modelo FCAPS para administración de redes.

FUENTE: Propio

❖ **Fault management**

Una falla dentro de una red es un evento con significado negativo, por lo que la meta de administración de fallas es reconocer, aislar, corregir y documentar sobre esta falla dentro de la red, luego es utilizado para analizar y predecir errores, lo que puede ser logrado estableciendo sistemas de monitoreo para prevenir el comportamiento anormal de la red.

❖ **Configuration management**

Las metas de la administración de configuraciones incluyen:

- Recolectar y almacenar configuraciones de los dispositivos de la red (esto se puede hacer localmente o remotamente).
- Simplificar la configuración de los dispositivos.
- Seguir los cambios que se realizan a la configuración.
- Configurar los circuitos o las trayectorias a través de redes no switchadas.

Pues las redes aumentan de tamaño, y una tarea importante es configuración automatizada. Algunos ejemplos de esta tarea son: DNS, RANCID histórico de cambios de configuración, manejo de archivos Cfengine, control de versiones RCS.

- **Accounting management**

  Accounting o manejo de contabilidad tiene como meta recopilar estadísticas de uso. RADIUS, TACACS y DIAMETER son ejemplos de los protocolos de uso general para manejo de cuentas. Las metas de la administración son controlar el sistema de usuarios autorizados estableciendo perfiles, contraseñas, permisos, y seguir las operaciones del equipo por ejemplo, realizando la reserva y la sincronización del software

  Implica seguir y controlar el uso de los recursos a los usuarios e informar a las autoridades sobre su apropiado uso y los costes que se asociaron a su utilización. Cuando son recursos escasos, puede ser necesario fijar límites en el uso de los mismos. Las acciones automáticas de corrección y limitación de uso para dichos recursos es una buena forma de administrar.

- **Performance management**

  La administración del desempeño permite al encargado preparar la red para el futuro, así como para determinar la eficacia de la red actual, por ejemplo, en lo referente a las inversiones hechas para instalarla. El funcionamiento de la red está enfocado en el rendimiento, porcentaje de utilización, detección de errores y tiempos de reacción. Recogiendo y analizando datos del funcionamiento, la salud de la red puede ser supervisada. Las tendencias pueden indicar la capacidad y la confiabilidad antes de que puedan afectar la calidad del servicio. Los umbrales del funcionamiento se pueden fijar para accionar alarmas.

- **Security management**

  La administración de seguridad debe reducir al mínimo el acceso desautorizado o accidental a las funciones de control de la red. Su función se ocupa de asegurar el legítimo uso de la información, el mantener, integridad de datos y auditoría. Debe proporcionar el control de acceso para la asociación, operación y notificaciones (alarmas de seguridad). De acuerdo con los derechos de acceso, debe habilitar o deshabilitar funcionalidades de los elementos de la red. Debe supervisar el sistema para cualquier ruptura de la seguridad y debe continuamente tomar automáticamente la acción correctiva como negar el acceso a algunas porciones de red o uso de funcionalidades.

8.1.ESTUDIO Y DISEÑO DE REGLAMENTOS PARA ADMINISTRACIÓN DE RED.

Los reglamentos administrativos son una parte importante para el correcto funcionamiento de una red tecnológicamente avanzada como la que posee Petroindustrial, por este motivo estos deben estar diseñados a la medida con el objetivo primordial de elevar su calidad y permitir un control muy estricto, a fin de preservar su desempeño y evitar fallas o problemas inesperados.

Los reglamentos deben aplicarse sobre cada uno de los servicios y recursos con el fin de controlar cada componente que conforma la estructura de la Red LAN de Petroindustrial. Así tenemos los siguientes:

8.1.1. **Reglamento para Uso del Servicio de Internet.**

El servicio de Internet que Petroecuador pone a disposición de los funcionarios de Petroindustrial, debe ser utilizado en base a un principio de responsabilidad de uso de un recurso limitado, de solidaridad y respeto con todos los usuarios que para cumplir con sus funciones también hacen uso del servicio, con este fin se establece el siguiente reglamento para su adecuado uso el cual incluye las siguientes normas:

- ✓ Dar prioridad a la navegación que busca enviar o recibir información necesaria relacionada con el trabajo que desempeña para la empresa, lo menos prioritario realizarlo en horas de menor congestión.

- ✓ No activar más de dos navegadores o ventanas de navegación simultáneas ya que esto crea sobrecargas al servicio.

- ✓ No bajar archivos o software en horas pico de operación, ya que provocan congestión en la Red, utilizar paquetes de software que le permiten hacer esta tarea en diferido, fuera del horario normal de trabajo.

- ✓ Procurar no enviar mensajes de e-mail con archivos de más de 200Kb de peso, ya que esto retardan el servicio de correo electrónico.

- ✓ No enviar un correo con archivos grandes a demasiadas personas, ya que el anexo se multiplica por cada una de los destinatarios a los que este enviando, ocasionando más trabajo para el servidor de mail y sobrecargando el ancho de banda usado para brindar este servicio.

- ✓ La Infraestructura tecnológica de Petroindustrial, cuenta con Filtrador de Páginas Web que permite registrar y administrar la navegación de cada usuario y por tanto bloquear el acceso a diferentes sitios, sin embargo aún cuando estuviera permitido no visite sitios no autorizados (ej.: sitios de sexo, chat, correos gratuitos como yahoo, hotmail, latinmail, canales de televisión y radios), esto eleva el consumo de nuestro canal de salida hacia internet.

- ✓ Petroecuador y Petroindustrial mantienen un sistema de monitoreo permanente, por tanto, si un usuario persiste en el acceso a enlaces prohibidos, el servicio le será bloqueado por completo y su restauración se deberá tramitar por escrito en el que se justifique la reincidencia y se haga el compromiso para respetar las normas establecidas.

- ✓ Cualquier consulta o sugerencia sobre el servicio de Internet, hacerla llegar al personal de la Unidad de Sistemas responsable de administrar este servicio.

8.1.2. **Norma para el Uso del Correo Electrónico.**

El servicio de Correo Electrónico que Petroindustrial pone a disposición de sus funcionarios, deber ser utilizado en base a un principio de responsabilidad de uso de un recurso destinado a facilitar la comunicación y coordinación necesarias para el cumplimiento de las actividades de trabajo, con este fin se establecen las siguientes normas para su correcto uso:

- ✓ Petroindustrial a través de la Red WAN, dispone del Servicio de Correo Electrónico en todas las Unidades Operativas de la Filial. .

- ✓ El buzón de correo de cada funcionario que dispone de este servicio, se encuentra en su equipo personal, por tanto a fin de mantener la configuración del mismo, debemos solicitar su respaldo cada vez que su PC es sometido a mantenimiento.

- ✓ Los recursos de comunicaciones y almacenamiento son limitados, por favor utilice el servicio para propósitos de trabajo, no está permitido enviar mensajes masivos con fines diferentes a todos los usuarios de la red. La reincidencia obligará a inhabilitar su cuenta de correo.

- ✓ Recuerde que a pesar de tener una cuenta personal, su dirección completa lo identifica como parte de Petroindustrial, por tanto del buen o mal uso de este recurso depende la imagen que proyectamos de nuestra Empresa.

- ✓ Procure no enviar mensajes con archivos de más de 200Kb ya que esto retarda el servicio de correo electrónico y ocasionará lentitud en los envíos.

- ✓ No envíe un correo con archivos grandes a demasiadas personas, ya que el anexo se multiplica por cada uno de los destinatarios a los que este enviando y esto aumenta el consumo de ancho de banda para terminar la tarea deteriorando el servicio para los demás usuarios.

8.1.3. **Acceso a equipos de Networking.**

Los equipos de networking instalados dentro de la red de Petroindustrial son dispositivos de funcionamiento crítico y por este motivo deben siempre estar protegidos de la manipulación tanto física como de lógica de cualquier persona extraña a los responsables de su administración y configuración. Por este motivo, se detallan las siguientes normas que deben aplicarse a fin de precautelar el correcto funcionamiento de los mismos, tanto en Petroindustrial Matriz como en las instalaciones de las refinerías.

- ✓ Los equipos de networking deberán estar correctamente asegurados dentro de su armario rack a fin de evitar golpes o caídas, así sean colocados por corto tiempo.

- ✓ No se deberá colocar ningún otro objeto sobre estos equipos, pues sus soportes de anclaje solo están diseñados para soportar el propio peso del mismo equipo.

- ✓ El armario rack debe estar correctamente energizado y poseer conexión a tierra a fin de evitar descargas eléctricas inapropiadas para el funcionamiento del equipo.

- ✓ El armario rack también debe poseer sistema seguridad (chapa), ventilación e iluminación adecuada y además de permitir la fácil manipulación de los equipos de networking, así como de los pach pannels de puntos de red instalados en el mismo.

- ✓ Los equipos de networking deben tener acceso restringido a su configuración, la misma que deberá estar protegida por su propio sistema de seguridad; y además las claves de acceso solo las deberá manejar única y exclusivamente el personal

de sistemas responsable, el mismo que por ningún motivo podrá proporcionarlas a personal ajeno.

- ✓ Si existen más de una persona que administra los equipos de networking, de preferencia se deberá manejar dentro de cada equipo el sistema de cuentas individualizadas (accounting) para poder mantener un registro lógico de quienes accedan a los equipos y que cambios realizan dentro de sus configuración.

- ✓ Cualquier cambio o novedad en alguno de los equipos deberá ser registrado en la bitácora de redes a fin de mantener un documento de respaldo acerca del funcionamiento de dichos dispositivos.

- ✓ Previo a realizar algún cambio de configuración dentro de alguno de los equipos de networking, se debe extraer un backup de la configuración a fin poder regresar a un estado de operación adecuado en caso de fallar la nueva configuración aplicada dentro del equipo.

- ✓ Si por algún motivo se necesita realizar cambios en la configuración de un equipo que afecte su normal funcionamiento y sea necesario reiniciarlo, este trabajo se lo deberá realizar de preferencia en las horas en que no haya usuarios activos, es decir fuera del horario normal de trabajo.

- ✓ En el caso de que el trabajo a realizarse, interrumpa el normal funcionamiento de la red en horas normales de trabajo, se deberá comunicar los usuarios de la suspensión de los servicios mediante los medios de comunicación masivos que posee la empresa. (Ej. E-mail, sistema de voces de la central telefónica).

8.1.4. **Normas de configuración de los equipos de Networking.**

La configuración de funcionamiento y operación de los equipos de networking de Petroindustrial es información sumamente valiosa e importante, por lo que debe ser manejada con mucho cuidado. Por este motivo se detalla un conjunto de normas para realizar una correcta configuración de estos dispositivos de forma que no afecte el rendimiento de la red o la operación de algún otro equipo.

- ✓ Configurar el equipo switch principal o Core como servidor de Tiempo, es decir hacer que este equipo sea el NTP MASTER de la red, de forma que sea el equipo con el que los demás switches deben sincronizarse a nivel de tiempo de operación.

- ✓ Configurar el equipo switch principal como servidor del Protocolo VTP (Vlan Trunk Protocol), dado que se tiene configurado redes virtuales y para fácil administración de estas, es mejor hacer que los demás switches sean clientes y hereden las configuraciones del equipo servidor VTP.

- ✓ Configurar en los equipos switches alternos que complementan el backbone el modo VTP en estado client, con el fin de que toda su información de Vlan's sea proporcionada por el switch de core.

- ✓ Cuando se instale otro equipo switch dentro de la red, siempre tener presente de realizar el cambio del modo VTP a transparent, de forma que su configuración de Vlan´s no sea propagada hacia el servidor VTP, y afecte la operación normal del switch de core.

- ✓ Cuando se añade un equipo switch nuevo a la red, se debe verificar que el número de revisión de configuración VTP sea menor al número registrado en el switch servidor VTP. Si es mayor, se debe cambiar al switch de dominio para volver ese número de revisión a cero de forma que no afecte a la configuración de vlan's establecida.

- ✓ Establecer, habilitar y configurar la seguridad de los puertos en cada switch de forma que solo se pueda conectar a la red el equipo PC registrado dentro de la configuración de cada equipo activo de red. Esta configuración es una norma de seguridad y debe contemplar el apagado del puerto si detecta la conexión de un equipo no registrado en la red.

- ✓ En los equipos Access Point wireless habilitar también el registro de equipos en la red por mac-address, de forma que solo se permita la conexión a los equipos pertenecientes a la red.

- ✓ Se debe incluir en la descripción de cada puerto de los switches el detalle de que punto de red le corresponde por conexión y en el mejor de los casos, añadir el nombre del PC conectado, sería de mucha utilidad en el caso de resolver problemas de comunicación.

8.2. APLICACIÓN DE LOS REGLAMENTOS PARA ADMINISTRACIÓN CON CISCOWORKS.

Para aplicar el sistema de reglamentos definido sobre esta herramienta de administración, como primer paso es poseer un "*Usuario*" y un "*Password*" para poder ingresar módulo de servicio de CiscoWorks; de preferencia esta clave debe ser de administrador o tener los permisos o roles necesarios para poder realizar cambios sobre las configuraciones de los equipos y demás parámetros de la aplicación.

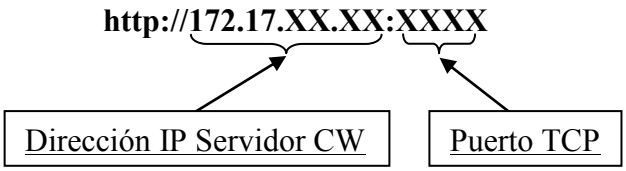
El acceder al Servidor de CiscoWorks es sumamente fácil para cualquier cliente, el cual debe contar con un sistema con requerimientos adecuados y un Navegador Web que soporte la aplicación como Netscape Navigator, Mozilla Firefox o Microsoft Internet Explorer versión 6.0 o superior. Además deberá tener instalado la máquina virtual de JAVA, muy necesaria para la ejecución de CiscoWorks, dado que este software basa toda su interface en esta tecnología. También se debe tener habilitado en el navegador de internet para que acepte cookies y ventanas temporales, pues la ejecución de las aplicaciones necesitan este requerimiento para funcionar correctamente.

Para acceder al Servidor CiscoWorks seguimos los siguientes pasos:

A. Se inicia un Navegador Web y se ingresa la URL del Servidor CiscoWorks seguido del número de Puerto de Conexión TCP : 1741, que es el Puerto de Conexión Default para el Web Server de CiscoWorks.

http://<Dirección IP o Nombre del Servidor>:<TCP_port>.

B. Para el caso de Petroindustrial se digita la dirección así:



C. Al terminar de cargarse el navegador, se mostrará una página Web con la Pantalla Inicial del Servidor CiscoWorks, Figura 8.1, donde se debe digitar el Usuario y el Password para iniciar una Sesión.

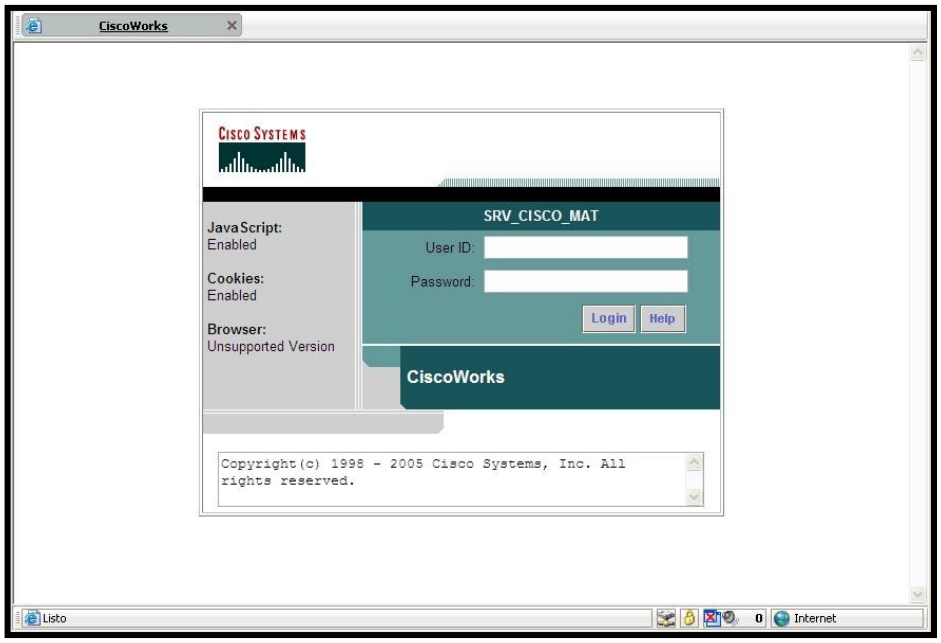


Fig: 8.2: Pantalla de Login de CiscoWorks.

FUENTE: Propio

D. Luego de realizar el ingreso aparecerá una nueva pantalla mostrando las diversas herramientas que dispone para la configuración, administración y monitoreo tanto de la interfaz de CiscoWorks como de los equipos de networking. Figura 8.2.

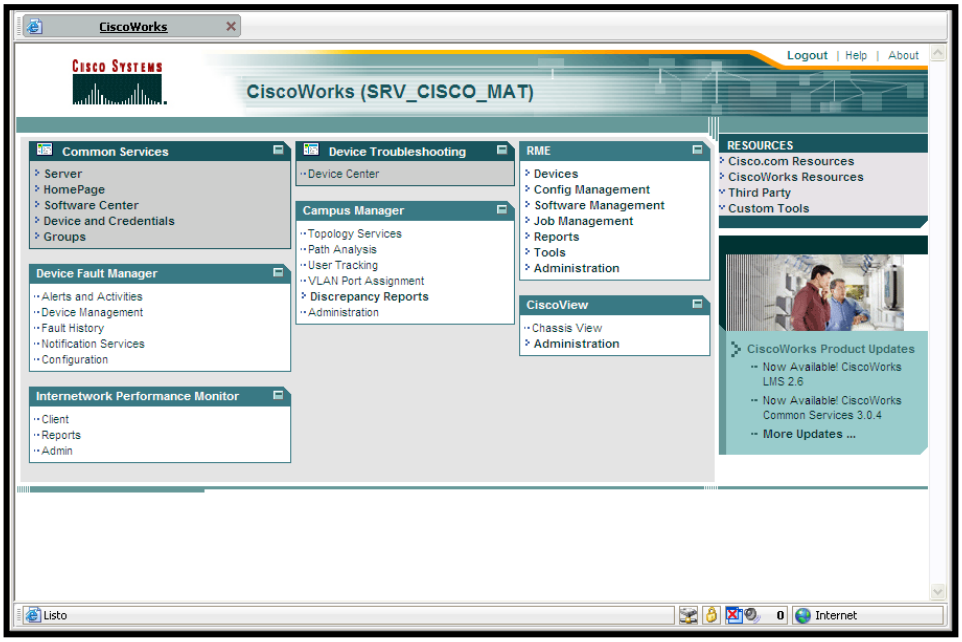


Fig: 8.3: Pantalla principal de administración de CiscoWorks.

FUENTE: Propio

E. Para realizar las diferentes actividades de administración y configuración, la pantalla de inicio de CiscoWorks proporciona de forma ordenada todas las herramientas de que está compuesta. A continuación se describen las herramientas por los números ubicados en la figura 8.4:

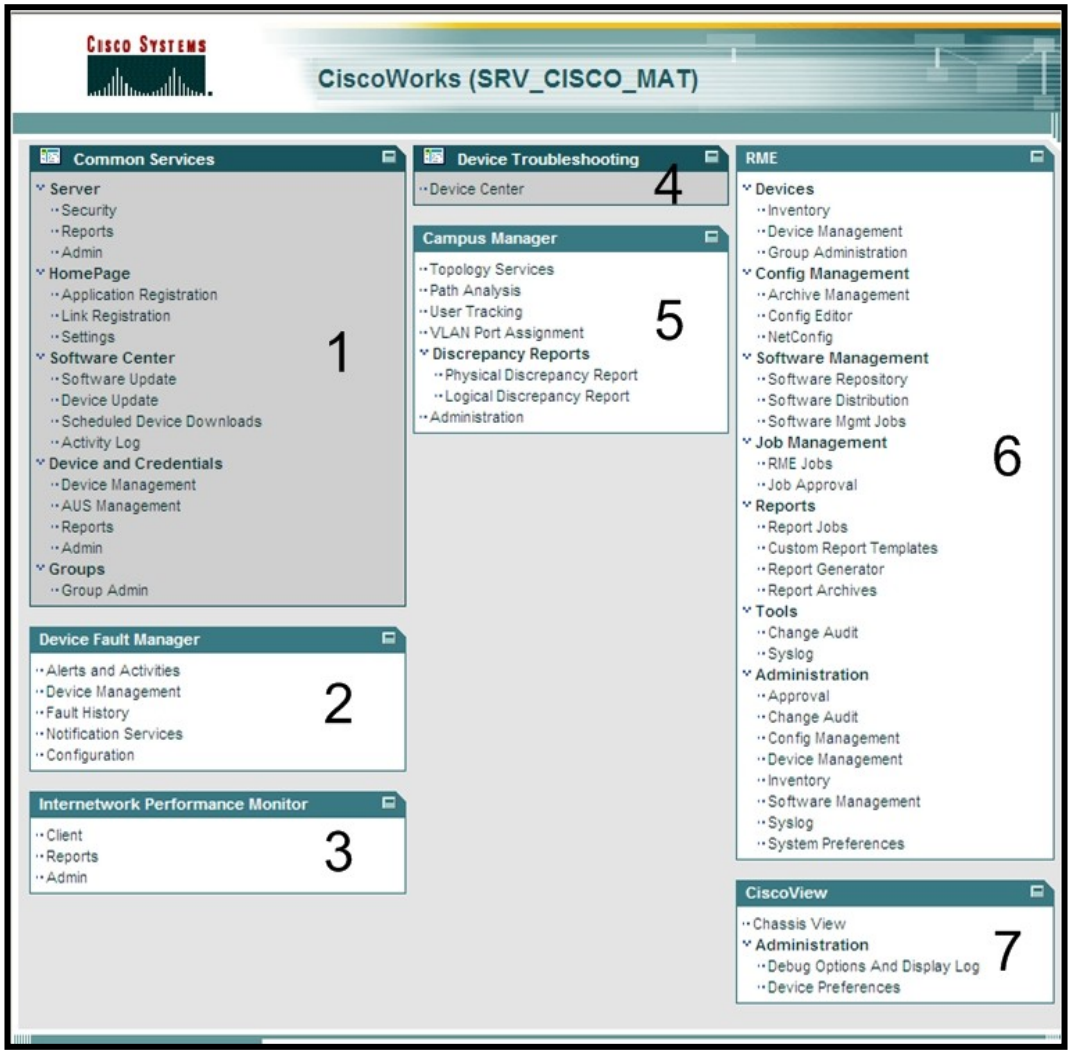


Fig: 8.4: Ubicación de herramientas de CiscoWorks

FUENTE: Propio

1. Common Services, módulo diseñado para configurar tanto el servidor de CiscoWorks, actualización de software y manejo de credenciales de los equipos de networking.

Fig: 8.5: Herramientas de Common Services.

FUENTE: Propio

2. Device Fault Manager, módulo diseñado para el manejo de fallas y solución de problemas.

Fig: 8.6: Módulo de Device Fault Manager.

FUENTE: Propio

3. Internetwork Performance Monitor, módulo creado para realizar el monitoreo de la red e implementar pruebas de generación de tráfico para comprobar el estado de operatividad de la red

Fig: 8.7: Módulo de Internetwork Performance Monitor.

FUENTE: Propio

4. Device Troubleshooting, modulo diseñado para solucionar problemas directamente relacionados con la operatividad de los equipos de networking.

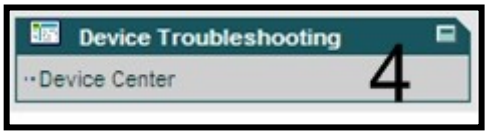


Fig: 8.8: Módulo de Device Troubleshooting.

FUENTE: Propio

5. Campus Manager, módulo diseñado para realizar vistas de la topología de la red, realizar pruebas de conectividad de los enlaces, configuración de Vlan's, así como discrepancias de funcionamiento dentro de los equipos de networking. También genera reporte de equipos conectados a los switches y administración topológica.

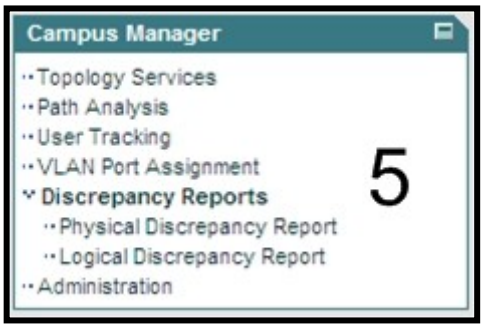


Fig: 8.9: Módulo de Campus Manager.

FUENTE: Propio

6. Resource Manager Esscentials, módulo diseñado para el manejo de inventario de dispositivos, administración de equipos, y grupos de administración. Permite también el manejo de archivos de configuración así como la edición de las configuraciones de los equipos. También permite manejar el inventario de software del sistema operativo de los equipos de networking, programar trabajos tales como actualizaciones. Permite realizar auditorías y llevar el historial de operación de los equipos.

Fig: 8.10: Módulo de Resource Manager Esscentials.

FUENTE: Propio

7. CiscoView, módulo diseñado para poder observar de forma gráfica los equipos de networking en la pantalla del PC y poder realizar algunas tareas de monitoreo y administración

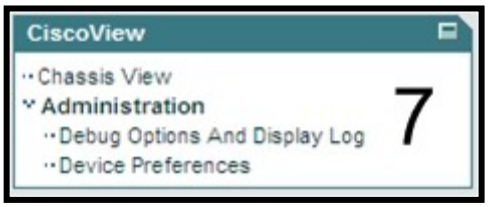


Fig: 8.11: Módulo de CiscoView.

FUENTE: Propio

F. Una vez que se ha ingresado al servidor, se debe habilitar las seguridades para el navegador, de esta forma se permitirá asegurar la privacidad, autenticación y la integridad de datos en todas las transacciones. SSL será el modo se seguridad que

se habilite en el servidor. Para esto se deberá acceder a la pantalla de Common Services, como lo indica la figura siguiente; y habilitar el Modo de Seguridad poniendo la casilla checkbox en ***Enable***, luego se presiona ***Apply*** y aparecerá una pantalla donde nos indica que para aplicar esta configuración es necesario reiniciar el servidor CiscoWorks.

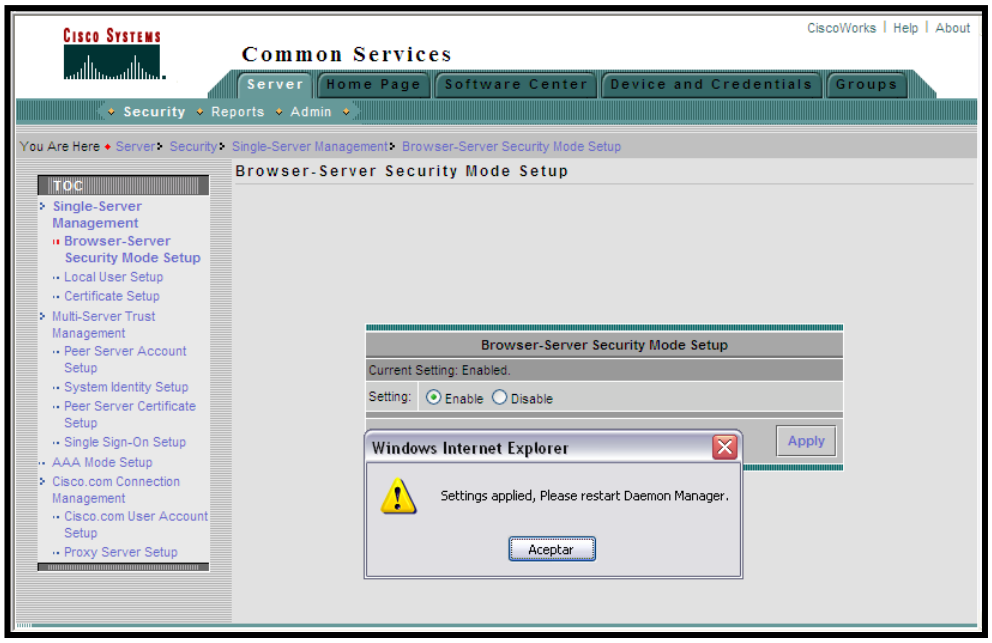


Fig: 8.12: Habilitando Modo de Seguridad SSL para el servidor CiscoWorks.

FUENTE: Propio

8.2.1. **Configurando Device Discovery**

Para poblar la base de datos de dispositivos, es necesario configurar y habilitar las credenciales de los equipos; siendo estas credenciales, atributos que deben poseer para poder ser administrados por CiscoWorks. Entre las credenciales solicitadas tenemos: usuario y password para modo privilegio de configuración; comunidades SNMP de lectura y escritura, sean estas en Versión 2 o 3 y opcionalmente usuario y password de HTTP.

Teniendo las credenciales a la mano, es hora de llenar la base de datos de dispositivos, para esto accedemos a la Administración de Campus Manager donde nos mostrará una pantalla indicando los parámetros utilizados para el descubrimiento de equipos. Ver figura siguiente.

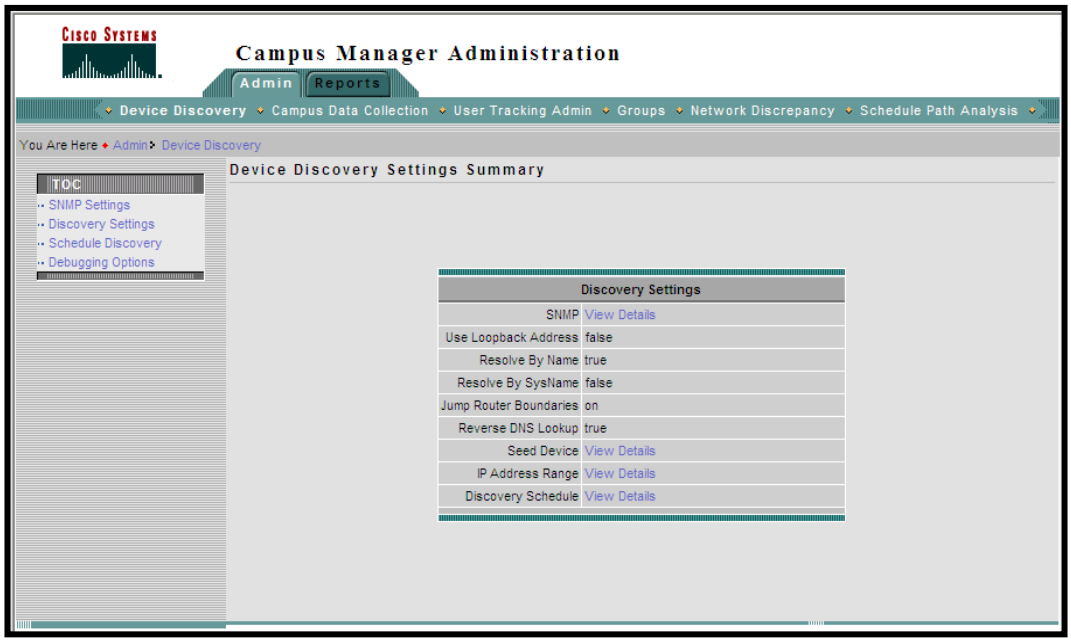


Fig: 8.13: Configuración de Campus Manager.

FUENTE: Propio

Accedemos entonces a ***SNMP Settings*** del panel izquierdo, donde ingresaremos las diferentes redes con las comunidades de SNMP especificadas en los dispositivos para que puedan ser descubiertos por la herramienta. Aparecerá un menú donde podremos ingresar los datos requeridos y ciertos parámetros con los que la configuración quedará completa. Para esto hacemos clic sobre ***Add***.

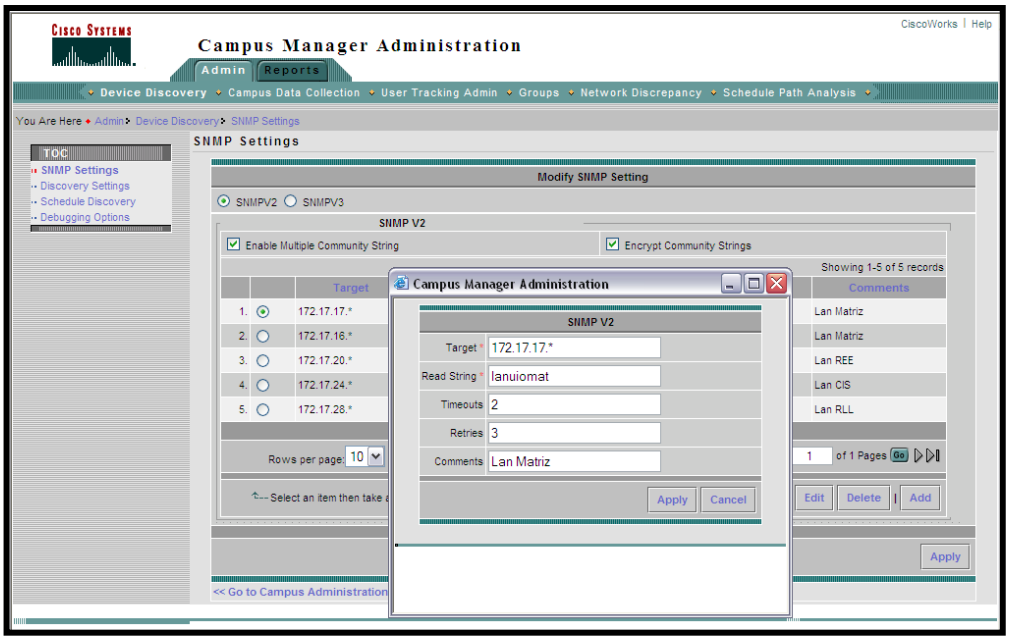


Fig: 8.14: Ingreso de Datos SNMP para descubrimiento de equipos.

FUENTE: Propio

Luego de ingresados los datos de descubrimiento, el menú nos permite modificar e incluso borrar los datos de alguna entrada que consideremos no necesaria a la hora de recolectar la información de los dispositivos de la red. Terminado el proceso de ingreso de parámetros, bastará con hacer clic sobre ***Apply*** para guardar los datos y hacer que el motor de descubrimiento empiece a trabajar. Ver figura 814.

Ahora tendremos que ingresar un dispositivo semilla o a su vez un rango de búsqueda de direcciones de red para que se ejecute el descubrimiento de equipos. La figura siguiente muestra como realizar el ingreso, para luego guardar los datos haciendo clic sobre ***Apply***.

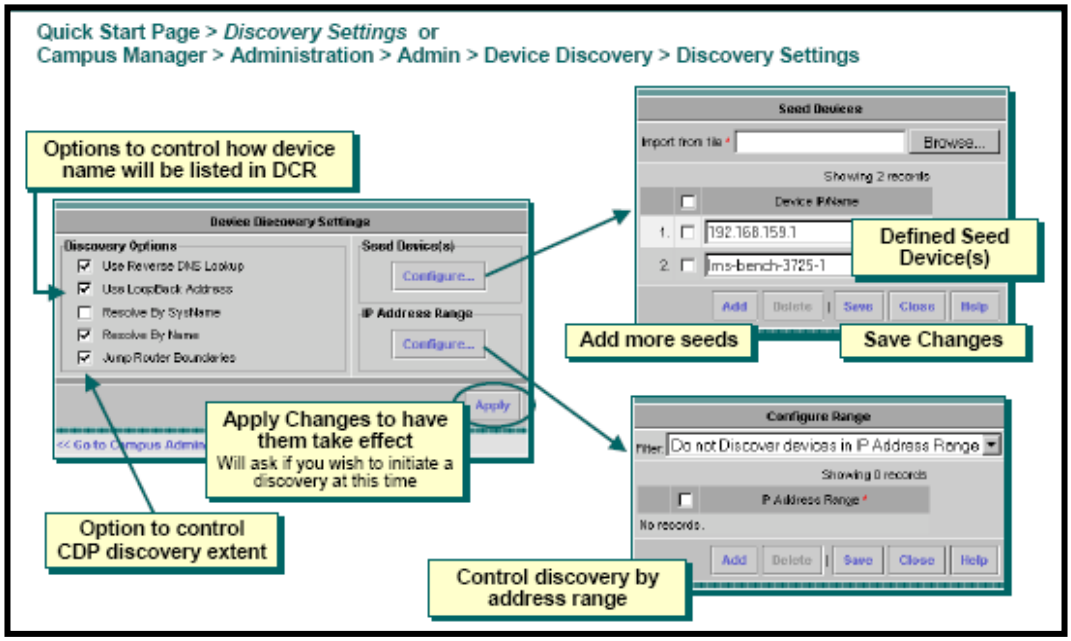


Fig: 8.15: Ingreso de dispositivo semilla ó rango de búsqueda de equipos en la red.

FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005, Pág.: 3-15

El siguiente parámetro a ingresar es el calendario de descubrimiento con el que se debe ejecutar la recolección de datos de los equipos dentro de la red. En la figura siguiente se muestra cuales son los calendarios establecidos los cuales pueden ser cambiados al gusto del administrador de red.

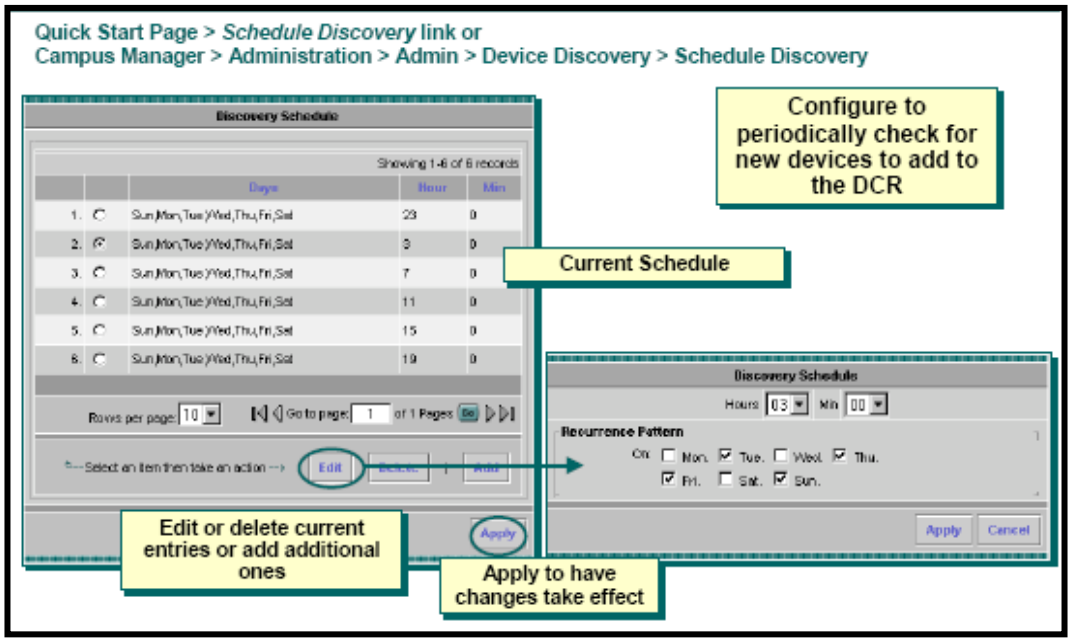


Fig: 8.16: Calendarizando el descubrimiento de equipos en la red.

FUENTE: CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005, Pág.: 3-16

Luego de ejecutado el ingreso de los parámetros de población de la base de datos de dispositivos, se puede generar un reporte de cuantos equipos han sido descubiertos, para lo cual accedemos a Campus Manager > Administration > Reports > Discovery Report, ver figura siguiente:

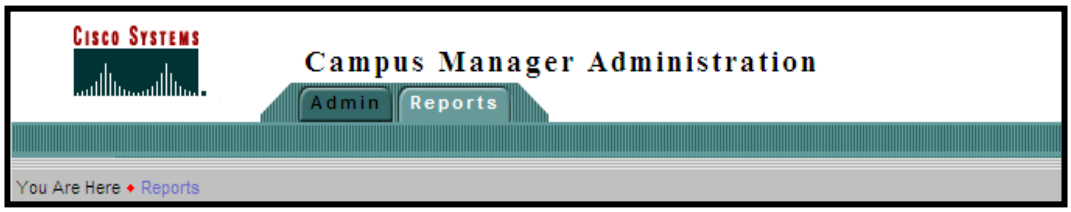


Fig: 8.17: Calendarizando el descubrimiento de equipos en la red.

FUENTE: Propio

En este nuevo menú debemos acceder a ***Discovery Report*** y luego hacer clic sobre ***Generate Report***, el cual nos mostrará el resultado de la búsqueda de equipos con las características de los mismos.

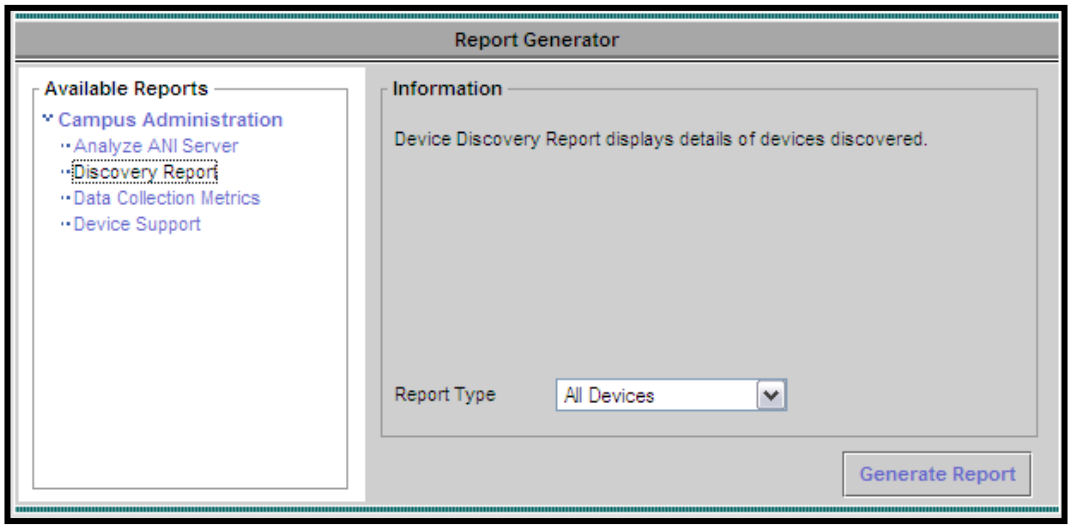
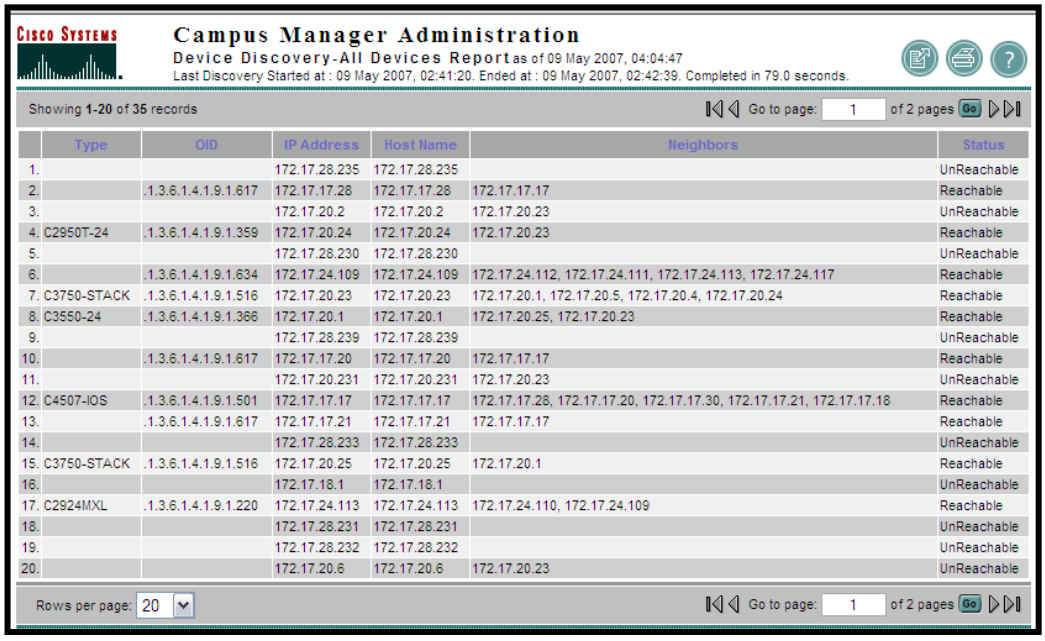


Fig: 8.18: Vista del generador de reportes de descubrimiento de equipos.

FUENTE: Propio

El resultado del reporte generado será el siguiente, el cual se muestra en la figura que sigue:



Campus Manager Administration

Device Discovery-All Devices Report as of 09 May 2007, 04:04:47

Last Discovery Started at : 09 May 2007, 02:41:20. Ended at : 09 May 2007, 02:42:39. Completed in 79.0 seconds.

Showing 1-20 of 35 records — Go to page: 1 of 2 pages

	Type	OID	IP Address	Host Name	Neighbors	Status
1.			172.17.28.235	172.17.28.235		UnReachable
2.		.1.3.6.1.4.1.9.1.617	172.17.17.28	172.17.17.28	172.17.17.17	Reachable
3.			172.17.20.2	172.17.20.2	172.17.20.23	UnReachable
4.	C2950T-24	.1.3.6.1.4.1.9.1.359	172.17.20.24	172.17.20.24	172.17.20.23	Reachable
5.			172.17.28.230	172.17.28.230		UnReachable
6.		.1.3.6.1.4.1.9.1.634	172.17.24.109	172.17.24.109	172.17.24.112, 172.17.24.111, 172.17.24.113, 172.17.24.117	Reachable
7.	C3750-STACK	.1.3.6.1.4.1.9.1.516	172.17.20.23	172.17.20.23	172.17.20.1, 172.17.20.5, 172.17.20.4, 172.17.20.24	Reachable
8.	C3550-24	.1.3.6.1.4.1.9.1.366	172.17.20.1	172.17.20.1	172.17.20.25, 172.17.20.23	Reachable
9.			172.17.28.239	172.17.28.239		UnReachable
10.		.1.3.6.1.4.1.9.1.617	172.17.17.20	172.17.17.20	172.17.17.17	Reachable
11.			172.17.20.231	172.17.20.231	172.17.20.23	UnReachable
12.	C4507-IOS	.1.3.6.1.4.1.9.1.501	172.17.17.17	172.17.17.17	172.17.17.28, 172.17.17.20, 172.17.17.30, 172.17.17.21, 172.17.17.18	Reachable
13.		.1.3.6.1.4.1.9.1.617	172.17.17.21	172.17.17.21	172.17.17.17	Reachable
14.			172.17.28.233	172.17.28.233		UnReachable
15.	C3750-STACK	.1.3.6.1.4.1.9.1.516	172.17.20.25	172.17.20.25	172.17.20.1	Reachable
16.			172.17.18.1	172.17.18.1		UnReachable
17.	C2924MXL	.1.3.6.1.4.1.9.1.220	172.17.24.113	172.17.24.113	172.17.24.110, 172.17.24.109	Reachable
18.			172.17.28.231	172.17.28.231		UnReachable
19.			172.17.28.232	172.17.28.232		UnReachable
20.			172.17.20.6	172.17.20.6	172.17.20.23	UnReachable

Rows per page: 20 — Go to page: 1 of 2 pages

Fig: 8.19: Reporte de equipos descubiertos dentro de la red.

FUENTE: Propio

Luego de que los dispositivos son registrados en la base de datos del DCR, están disponibles para los demás paquetes de administración de CiscoWorks, permitiendo su administración y control.

8.2.2. **Generación de reportes de dispositivos**

Para generar un reporte del inventario de dispositivos que se han detectado dentro de la red, con las especificaciones y características de cada uno, seguimos los siguientes pasos: RME > Reports > Report Generator; como nos muestra la figura siguiente. Luego tendremos que seleccionar el tipo de reporte y que características vamos a solicitar.

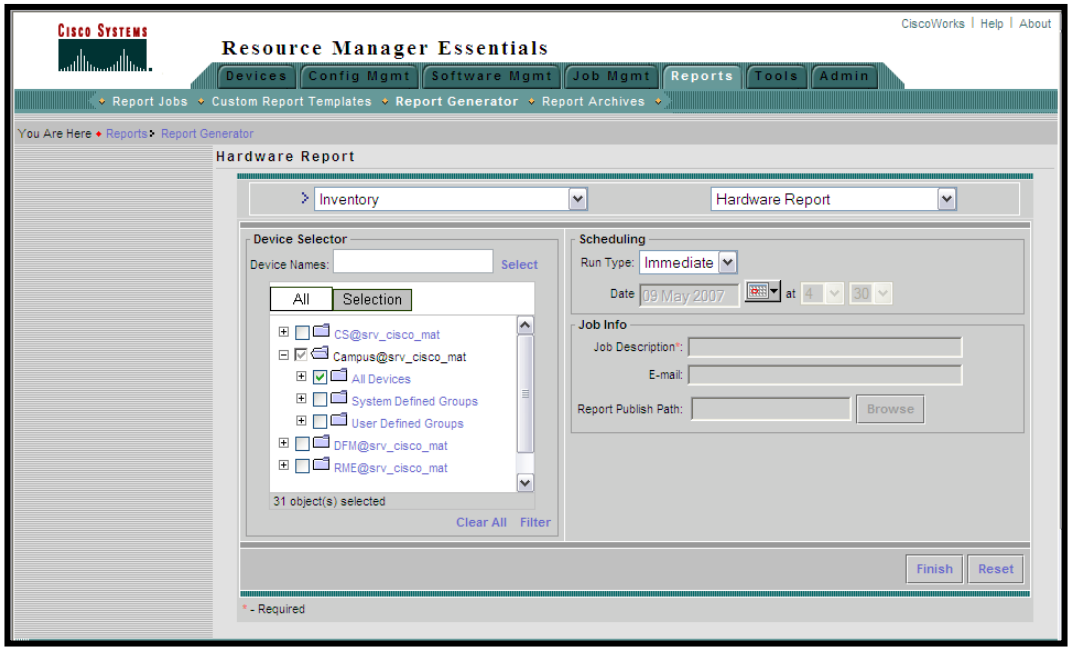


Fig: 8.20: Habilitando Modo de Seguridad SSL para el servidor CiscoWorks.

FUENTE: Propio

Seleccionadas las opciones, bastará con hacer clic sobre ***Finish*** para que nuestro reporte se genere.

Si se desea generar nuevos reportes, con otro tipo de criterios, como Inventario de cambios sobre algunos equipos, auditorias, detalles del chasis, versión de software; se deberá elegir las opciones adecuadas como lo muestra la figura anterior. Este generador de reportes es muy útil y eficiente facilitando así, un sin número de tareas que antes se debía realizar a mano y que involucran mucho tiempo. La figura siguiente muestra uno de los reportes que fue generado con esta herramienta.

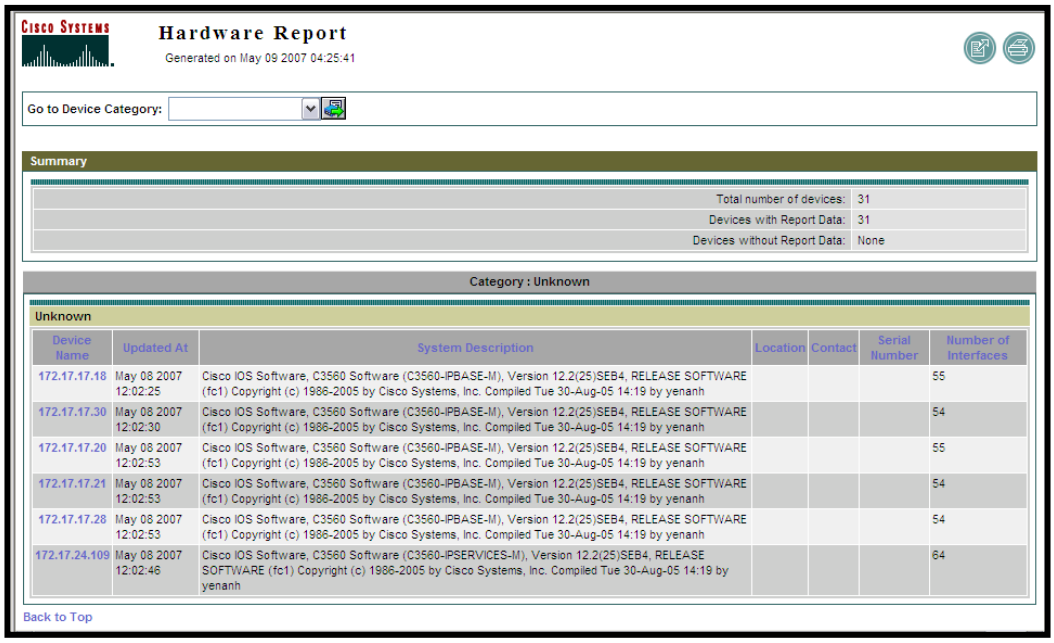


Fig: 8.21: Reporte de inventario de Hardware de los equipos detectados dentro de la red.

FUENTE: Propio

8.2.3. **Administrado equipos con Campus Manager**

Campus Manager es un conjunto de herramientas muy eficientes que permiten la administración de los equipos, hacer pruebas de conectividad y además de eso observar la topología de los dispositivos dentro de la red. Para esto accedemos hasta Campus Manager > Topology Services. Aparecerá una ventana con el detalle de los dominios que reconoce dentro de la red luego de la detección de dispositivos.

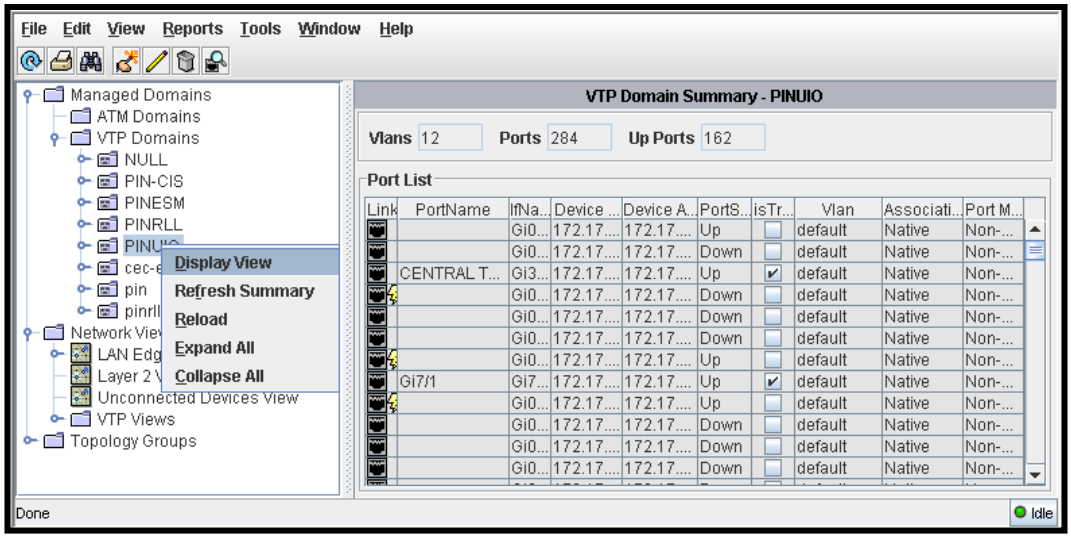


Fig: 8.22: Ventana de información de Topology Services de CampusManager.

FUENTE: Propio

Terminada la carga de la ventana aparecerá el detalle de los dispositivos detectados sobre la red, además de la topología y los dominios de VTP que se han encontrado. Al hacer clic derecho con el mouse podemos acceder al despliegue de la vista, el cual nos mostrará la topología gráfica de dicho domino observado

En la siguiente figura se muestra la información topológica del domino VTP PINUIO, al ser detectada por Campus Manager

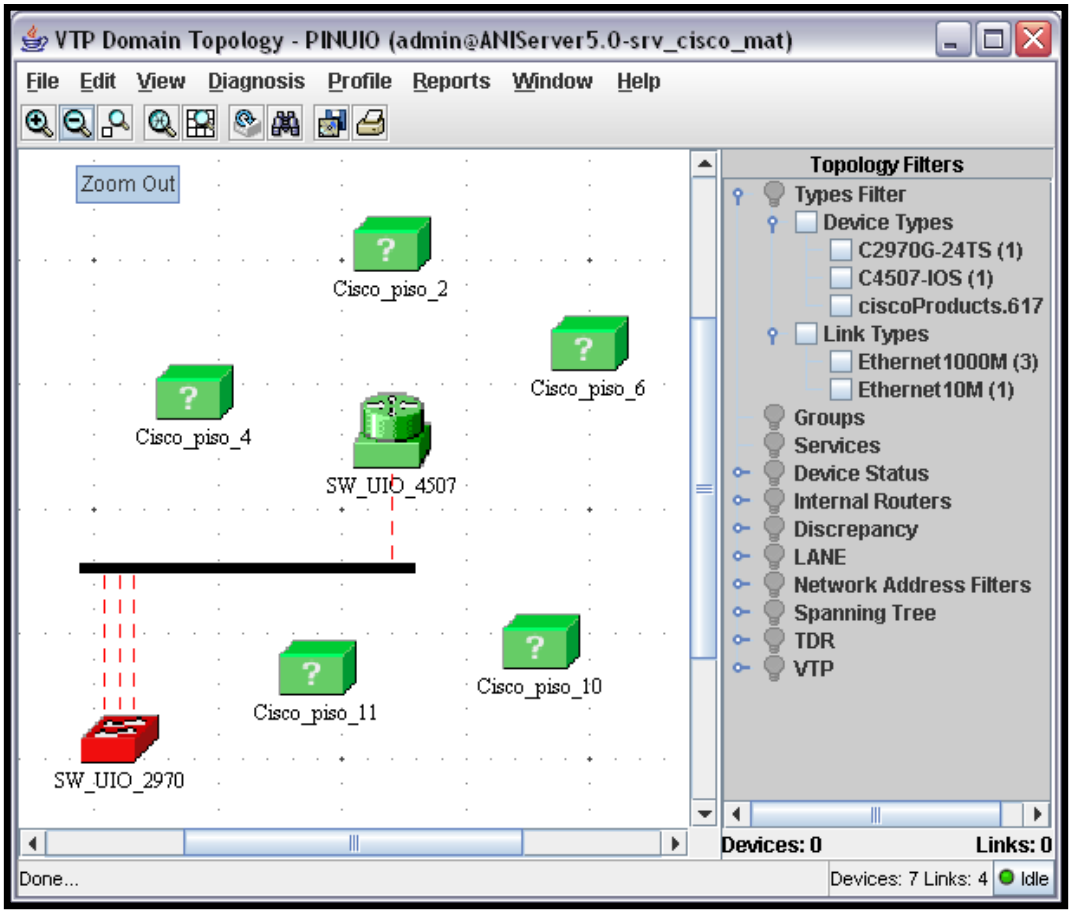


Fig: 8.23: Detalle del Topology Services de un dominio VTP detectado por Campus Manager.

FUENTE: Propio

En esta vista se puede identificar el equipos principal de core y los alternos del backbone de fibra óptica. El detalle faltante de la conectividad entre los dispositivos está dada por la falta de actualización de IDUs de los equipos Cisco dentro del servidor de CiscoWorks, esta actualización se la realiza mediante el acceso a la página Cisco Conection Online bajo contrato de Smartnet.

Dentro de la pantalla de Topology Services podemos ver en el panel derecho los puertos de los equipos cisco dentro de un dominio VTP a su vez al hacer clic derecho con el mouse, se puede tener acceso a varias opciones adicionales que permiten configuración y manejo tanto de dichos puertos como del mismo dispositivo en sí. En la figura siguiente, se muestra CiscoView invocado desde Topology Services.

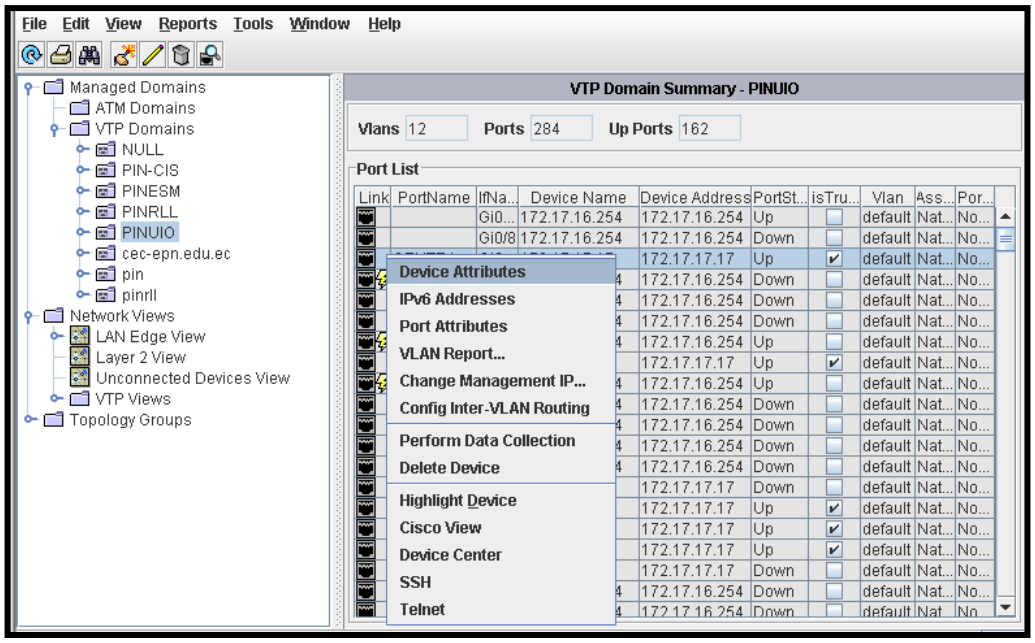


Fig: 8.24: Opciones de administración ofrecidas desde Topology Services.

FUENTE: Propio

Además de ofrecer un detalle de los puertos que posee cada dispositivo, se puede obtener algunas opciones de administración que invocan a las herramientas correspondientes para realizar este propósito. Es aquí donde se ve la versatilidad de la herramienta en la manipulación de los dispositivos y sus configuraciones.

Otra forma de acceder a las configuraciones es desde Device Center de Device Troubleshooting, el mismo que ofrece un amplio conjunto de herramientas que están destinadas para la administración y configuración de los dispositivos ubicados en la base de datos de Cisco Works. Ver figura 8.27.

De la misma forma, Cisco View permite la configuración de ciertos parámetros sobre la imagen real del dispositivo. Entre esas opciones de administración son limitadas en esta vista. Ver figura 8.26.

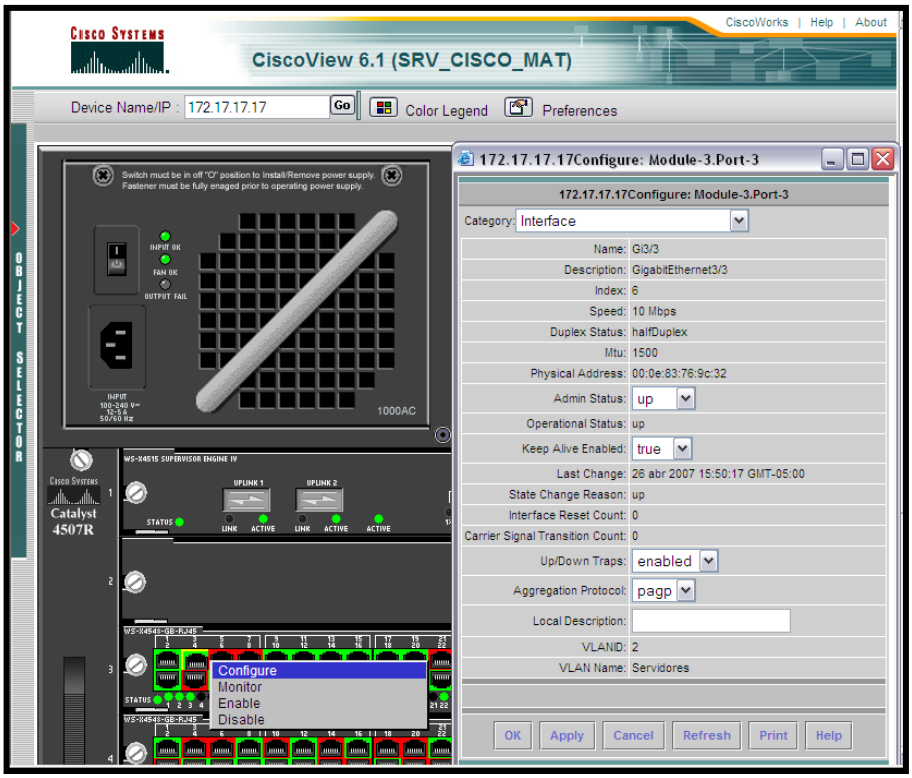


Fig: 8.26: Opciones de configuración sobre Cisco View de CiscoWorks.

FUENTE: Propio

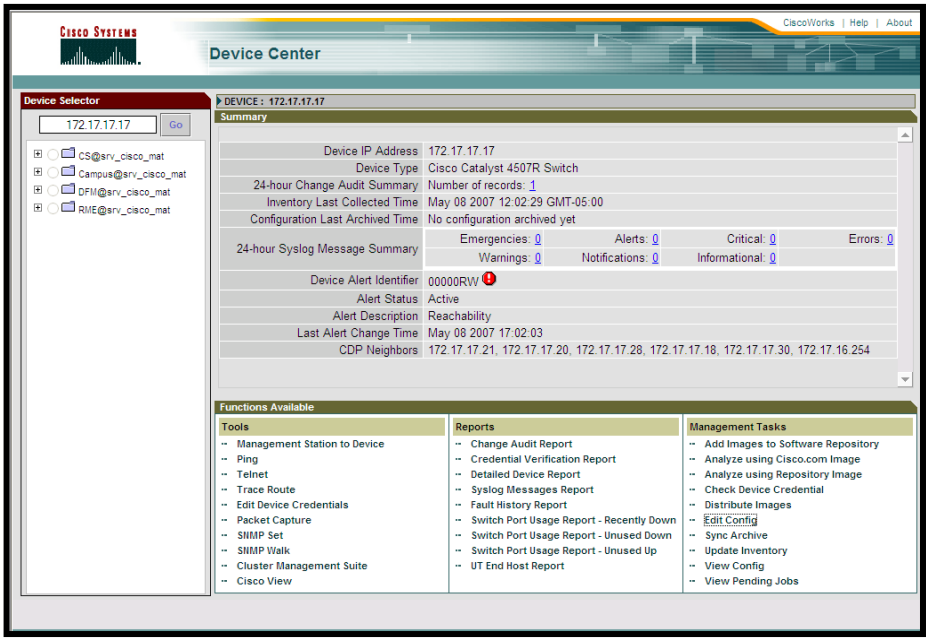


Fig: 8.27: Device Centre ofrece más opciones de administración y monitoreo de los dispositivos.

FUENTE: Propio

8.3.REGLAMENTACIÓN DE USO DE SERVICIOS Y RECURSOS DE RED UTILIZANDO CISCOWORKS.

8.3.1. POLÍTICAS DE SEGURIDAD

La evolución de las nuevas tecnologías, en especial el tremendo auge de las tecnologías Internet/Intranet y correo electrónico, han provocado la aparición de nuevas necesidades y la posibilidad de adquirir ventajas competitivas.

Los beneficios atribuibles a las nuevas tecnologías son muchos, pero también los riesgos: La pérdida de imagen (a menudo más crítica que la propia pérdida de datos), la pérdida de información, la suplantación de usuarios y el espionaje.

A pesar de lo cambiante del entorno, los requisitos de seguridad siguen siendo los mismos: Autenticación, confidencialidad, control de acceso e integridad. En un mundo cada vez más dependiente de las redes, es vital no sólo proteger el acceso a los recursos de los 'malos', sino también evitar una manipulación accidental con fatales consecuencias.

El implementar políticas de seguridad es una excelente práctica y un requerimiento para disminuir múltiples factores de riesgo como el acceso desautorizado o inadvertido a recursos de la red así como minimizar el soporte técnico.

8.3.1.1. La problemática de seguridad

A lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas, han sido una constante recurrente que tiene su origen en la falta de definiciones estructurales y tecnológicas que se apliquen a todo nivel.

- Habitualmente la estructura de la organización no se hace pensando en la seguridad por lo que no hay una definición formal de las funciones ni responsabilidades relativas a seguridad.

- No suelen existir canales de comunicación adecuados para tratar incidentes de seguridad, predominando los canales de tipo informal.

- Exceptuando determinados ambientes como la banca o la defensa, no suelen existir recursos específicos dedicados a seguridad, y cuando existen suelen dedicarse a la seguridad física (puertas, alarmas, dispositivos contra incendios, etc.) por ser más fácilmente justificable su adquisición.

- Habitualmente las directrices no son homogéneas en toda la organización.

- Como consecuencia de la falta de definición de funciones, nadie quiere responsabilizarse de los riesgos asumidos en la organización y nadie quiere adoptar medidas que puedan dificultar la operación normal de las actividades de la Empresa.

- No se definen normas ni procedimientos salvo cuando su ausencia puede afectar al propio negocio (por ejemplo la existencia de copias de seguridad) o tras un incidente grave de seguridad.

- Al no existir beneficios inmediatos, resulta difícil justificar gastos y recursos.

- Las herramientas existentes son un soporte y por sí solas no cubren todas las necesidades de seguridad. Se constituyen en el apoyo de las normativas definidas para minimizar riesgos.

8.3.1.2. Análisis de riesgos

Durante el tiempo de operación de la red WAN de Petroindustrial se han identificado distintos factores de riesgo que pueden desencadenar un desastre total o parcial en su funcionamiento.

La importancia de identificar estos riesgos radica en tomar correctivos para su prevención o minimizar su efecto y cuantificar la pérdida económica que la Empresa sufriría si el servicio que la red presta se interrumpe por algún tiempo significativo.

Los factores de riegos más relevantes identificados dentro de la red LAN y WAN de Petroindustrial son:

La ocurrencia de estos riesgos dentro de la red LAN y WAN de Petroindustrial generaría la suspensión total o parcial del servicio de correo electrónico, navegación en internet, el normal funcionamiento de las aplicaciones que operan localmente y/o que son utilizadas en forma remota desde la Matriz.

N°	FACTORES DE RIESGO	NIVEL DE RIESGO
1	Falla permanente de los enlaces de comunicación vía microonda	Medio
2	Falla de los equipos de enrutamiento y/o networking	Alto
3	Ataques por virus o intrusos desde internet	Alto
4	Fuego	Bajo
5	Robo común	Medio
6	Fallas en los equipos PC, daño de información	Medio
7	Errores humanos que dañen información	Bajo
8	Desastres naturales que destruyen archivos y equipos	Bajo
9	Accesos no autorizados, robo de información	Medio
10	Accesos remotos no autorizados	Medio
11	Instalación de software no licenciado	Alto

Tabla 8.1: Factores de riesgo dentro la red de LAN y WAN de Petroindustrial

FUENTE: POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA RED INTEGRAL DE INFORMACIÓN DE PETROINDUSTRIAL

8.3.1.3. Seguridad implementada actualmente

Los sistemas de seguridad y protección que la Unidad de Sistemas ha implementado hasta el momento tratan de establecer un nivel de seguridad básico. Esta temática se encuentra en constante revisión a fin de mejorar cada día más e ir cubriendo y eliminando las fallas de seguridad.

A nivel de los equipos activos de red marca Cisco y Motorola se cuenta con los siguientes procesos de seguridad enfocados en la prevención y protección:

- El acceso a los equipos en modo de ejecución, modo de privilegio y modo de configuración global está controlado por el servicio de encripción de claves que posee el sistema operativo IOS de los mismos equipos.

- Las claves son manejadas únicamente por el administrador de los equipos de networking y son frecuentemente cambiadas para evitar posibles robos de las mismas.

- La administración de la red local se facilita con la configuración e implantación de redes virtuales Vlan's que permite separar en pequeños conjuntos de red toda la infraestructura tecnológica y aislar las fallas para su pronta solución.

- El acceso no autorizado se encuentra controlado con la implementación de ACL's en el enrutador-switch principal 4507R. Este tipo de filtrado es aplicado para evitar el ingreso de intrusos a la red de Petroindustrial.

- La implementación del protocolo Frame Relay se realizó en los equipos de enrutamiento marca Vanguard instalados en las cuatro Unidades operativas de la Filial. De esta forma se permite el enrutamiento de datos y voz por el mismo canal de comunicación facilitando así la interconectividad entre los distritos.

- Los equipos de networking que están instalados en los pisos del edificio se encuentran dentro de armarios racks que poseen seguridades y ventilación apropiada para su operación. Las llaves de estos armarios las tiene únicamente el administrador de estos equipos.

- Los equipos enrutador switch Cisco 4507 y Vanguard Motorola 6455 se encuentran instalados en el Centro de Cómputo dentro del piso de la Unidad de Sistemas, el mismo que cuenta con sistema de seguridad biométrico, aire acondicionado y sistema contra incendios.

8.3.1.4. Respaldos de configuraciones de equipos de Networking.

El backup del sistema operativo y configuraciones de todos los equipos Cisco a nivel nacional se realiza de forma automatizada mediante la herramienta de Administración CiscoWorks según la tabla siguiente.

CONTENIDO DEL BACKUP	PERIODICIDAD
Backup del IOS de los equipos	Trimestralmente
Backup de las configuraciones	Mensualmente

Tabla 8.2 Calendario de backups de equipos de networking

FUENTE: POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA RED INTEGRAL DE INFORMACIÓN DE PETROINDUSTRIAL

En el caso de realizarse alguna modificación en las configuraciones se realiza un backup previo a los cambios y es almacenado en medios magnéticos (CD's).

Para el equipo enrutador Vanguard Motorola, dado que se encuentra bajo la responsabilidad operativa del personal técnico de Petrocomercial, los respaldos de su sistema operativo y de archivos de configuración lo realizan bajo sus normas de backup pero que se apega a los reglamentos establecidos en Petroindustrial.

8.3.2. NORMATIVA Y PROCEDIMIENTOS

Si bien la falta de control sobre la información es un riesgo latente, se ve difícil la materialización del mismo en un momento dado.

No se puede valorar el efecto que producirá en un tercero una determinada información. Por ello, toda la información debe ser objeto de protección frente a fugas incontroladas o robos premeditados.

Ningún sistema de seguridad puede garantizar un cien por cien de eficacia, ni tampoco se puede llevar la seguridad hasta extremos de paranoia que imposibiliten el normal funcionamiento de la Empresa.

Es por eso que se hace necesario establecer normas de seguridad en el tratamiento de la información que garanticen la correcta utilización de la misma.

8.3.2.1. Seguridad Física del Centro de Cómputo

El centro de cómputo es el área física donde reside más del 90% de la información que se maneja en forma autorizada, es por ello, que merece ocuparse de él en primer lugar.

Las principales normas a tener presente son las siguientes:

- La sala debe reunir requisitos mínimos de aislamiento a altas temperaturas, humedad, fallas en los circuitos eléctricos, etc.

- En caso de que la sala linde con el exterior debe proveerse de cortinas y cerraduras interiores de ventanas y puertas que mantengan una seguridad física adecuada.

- Evitar los daños por agua que pueden ocurrir como resultado de goteos del techo y goteos de tuberías que atraviesen el centro de cómputo.

- Sellar o proteger todas las tuberías abiertas que permitan el paso de roedores o cualquier otro tipo de animales desde el exterior.

- Evitar el humo y polvo, que son frecuentemente introducidos en el centro de cómputo, a través del sistema de aire acondicionado.

- Contar con sistemas de alarmas y dispositivos contra incendios del tipo GAS CARBÓNICO (CO2) o FM200, que nos permita actuar con rapidez y sofocar un incendio para prevenir el deterioro o destrucción de los equipos y la información.

- Eliminar las interferencias electromagnéticas y de radio frecuencia, es decir, los ruidos eléctricos que interfieren en el funcionamiento de los componentes electrónicos del servidor y ponen en peligro la integridad de los datos.

- Proteger a los equipos instalados en el Centro de cómputo, garantizando que exista ventilación permanentemente en el área.

- El acceso a esta área estará restringida al ingreso exclusivo del Administrador y Operador, se deberá identificar claramente con letreros la prohibición de acceso a personal no autorizado.

- Instalar un sistema de control de acceso que permita registrar quienes ingresan, en que horario y permita restringir el ingreso de personal no autorizado.

- Todas los toma corrientes que suministren energía eléctrica a los servidores del centro de cómputo deberán estar aterrizados e integrados al UPS central.

- Los servidores deben ubicarse sobre mesas de aislamiento que impidan daños por movimientos.

8.3.2.2. Procedimientos operativos

Establecer una bitácora de operación de los equipos de networking; en ella se documentarán las actividades relevantes ejecutadas sobre ellos, de la misma manera se registrarán las acciones tomadas para superar emergencias. Por disposición de la Jefatura de la Unidad de Sistemas, mediante memorando 781-PIN-SIS-2004, del 21 de Diciembre del 2004, la información mínima por cada atención o problema que debe registrarse en las bitácoras es la siguiente:

- Fecha y Hora del evento
- Responsable de la revisión
- Descripción del Problema
- Causa(s)
- Usuario responsable
- Solución(es)
- Acciones preventivas a tomar para el futuro.

8.4.ANÁLISIS DE SERVICIOS Y RECURSOS A MONITOREAR DENTRO DE LA RED.

Dentro de los Servicios y Recursos destinados para monitorear y obtener un mejor desempeño de la Red LAN y WAN de Petroindustrial se han considerado los siguientes como más importantes y críticos.

8.4.1. **Servicios a Monitorear dentro de la red.**

Dentro de los servicios a monitorear tenemos los siguientes:

- Servicio de correo electrónico.
- Servicio de navegación en internet.
- El uso de recursos de red compartidos.
- Acceso a servidores para aplicaciones específicas
- Acceso a aplicaciones que demanden alto ancho de banda.

8.4.2. **Recursos a Monitorear dentro de la red.**

Dentro de estos equipos se considera primordial tanto a nivel de Petroindustrial Matriz como de sus Refinerías el monitoreo permanente de todos los equipos ruteadores, switches, radios y Access Point administrables, dado que su correcta operatividad permitirá evitar posibles fallas, errores de comunicación, caídas de enlaces y micro-cortes que afecte el desempeño de la red LAN y WAN.

El monitoreo deberá incluir tanto una revisión física como de configuración y logs de errores, con el fin de mantener el equipo en el mejor estado posible y prevenir fallas inesperadas.

Se deberá monitorear las interfaces principales de operación dentro de estos equipos a fin de detectar accesos indebidos, uso inadecuado de recursos o protocolos y ancho de banda de consumo.

Además se debe también montar un Sniffer, de forma que permita tener una referencia de cómo se muestra el trafico sobre la infraestructura de la red actualmente, enfocándose también sobre el monitoreo de protocolos como HTTP, FTP, TFT, SMTP, SNMP, para así definir o reestructurar normas que permitan controlar o manejar de mejor manera el trafico detectado sobre la red, sea esta LAN o WAN.

8.5. IMPLEMENTACIÓN DE MONITOREO SOBRE LA RED LAN Y WAN DE PETROINDUSTRIAL CON CISCOWORKS.

Para implementar el monitoreo sobre los equipos activos de la red LAN y WAN de Petroindustrial mediante CiscoWorks debemos realizar los siguientes pasos:

8.5.1. Verificación de credenciales de los dispositivos.

En este caso de deberá acceder al Common Services y seguir los pasos como muestra la figura 8.12, seleccionamos los equipos y escogemos en el menú inferior ***Edit*** que abrirá un asistente para ingresar y actualizar los datos de las credenciales de cada dispositivo.

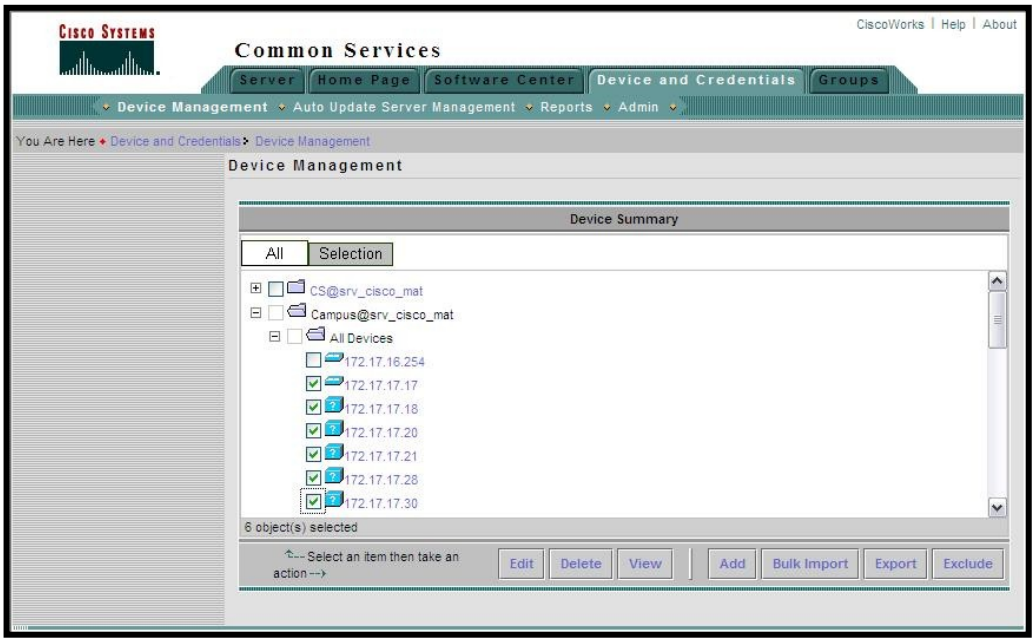


Fig: 8.28: Actualización de credenciales para dispositivos a monitorear.

FUENTE: Propio

En el asistente debemos seleccionar uno por uno los equipos a actualizar y presionar el botón ***Next*** para continuar el proceso. Figura 8.13.

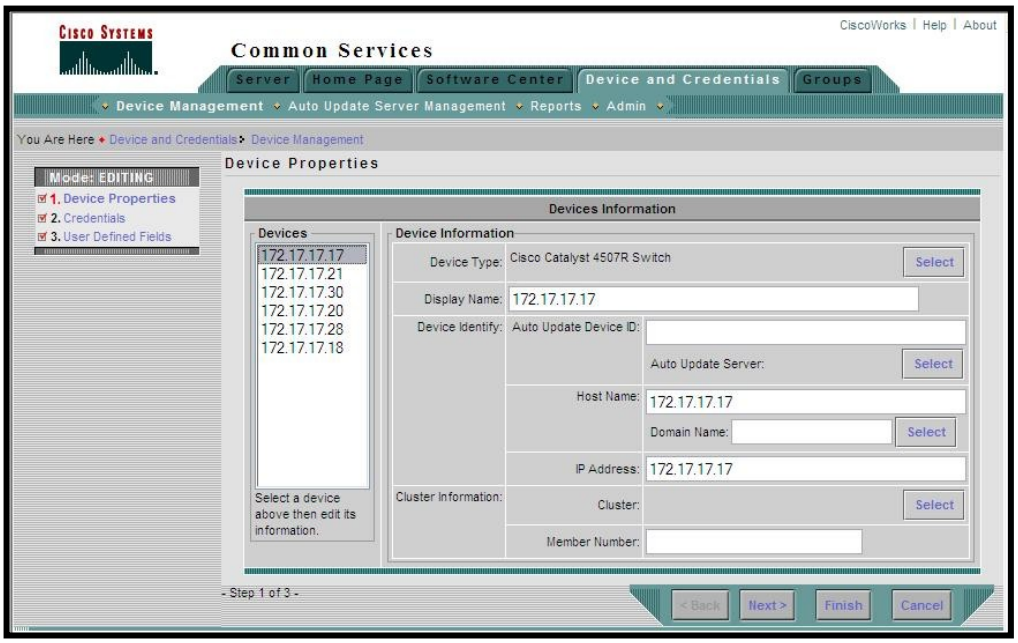


Fig: 8.29: Asistente para actualización de credenciales para dispositivos a monitorear.

FUENTE: Propio

Se ingresarán los valores solicitados por el asistente y presionará el botón de ***Next*** para continuar el proceso.

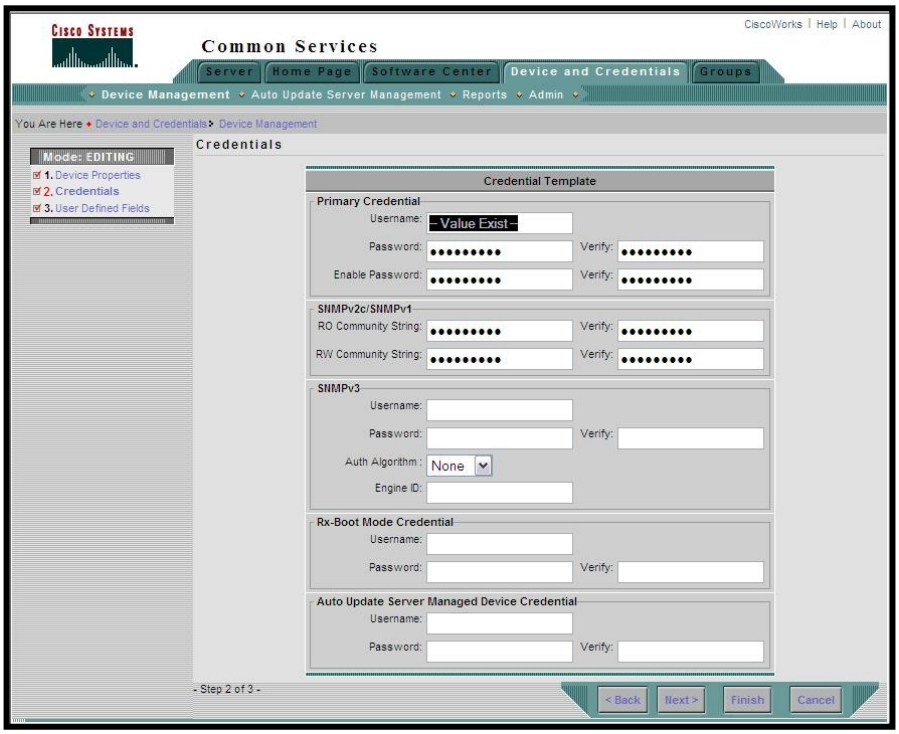


Fig: 8.30: Actualización de credenciales para dispositivos a monitorear.

FUENTE: Propio

En la siguiente pantalla del asistente solicita otro tipo de información la cual no es necesario ingresarla, solo hará falta hacer clic sobre el botón de ***Finish*** para terminar el proceso de actualización de credenciales. Este procedimiento se lo debe realizar para cada equipo, de forma que se permita a la herramienta el acceso a la configuración de los equipos y permita administrarlos

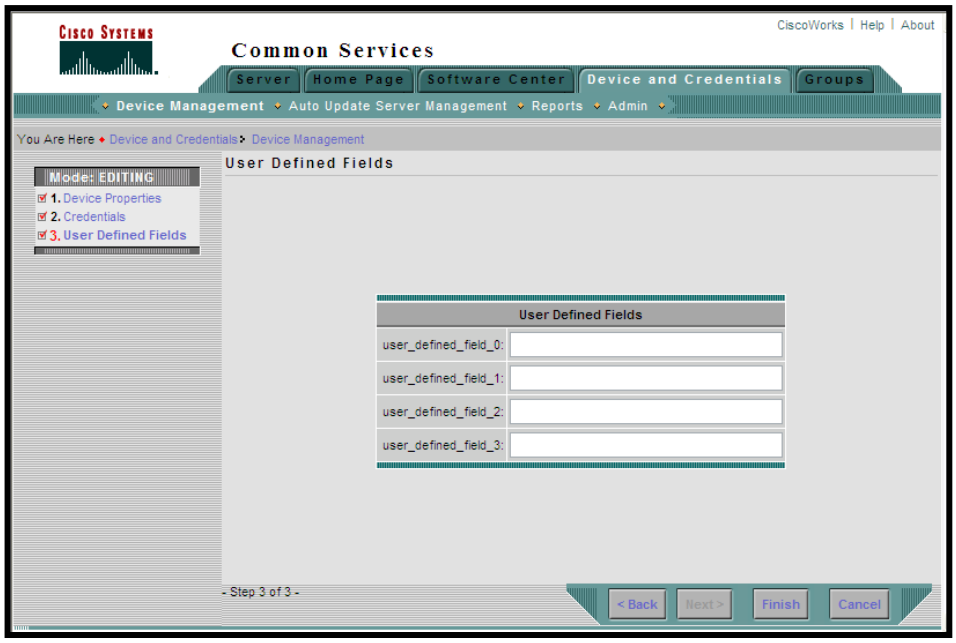


Fig: 8.31 Actualización de credenciales para dispositivos a monitorear.

FUENTE: Propio

8.5.2. **Importando los dispositivos para monitorear**

Para iniciar el monitoreo debemos seguir la pantalla siguiente de Internetwork Performace Monitor tal como lo muestra la figura siguiente, a fin de incluir los dispositivos dentro del listado de equipos a ser monitoreados. Nos pedirá que escojamos el origen de donde deseamos importar los dispositivos, en este caso elegiremos ***Source***, que es el origen de datos de CiscoWorks y donde se almacena todas las credenciales y configuraciones de acceso para los dispositivos administrados por esta herramienta. Luego presionamos el botón de ***OK*** para iniciar el proceso de importación.

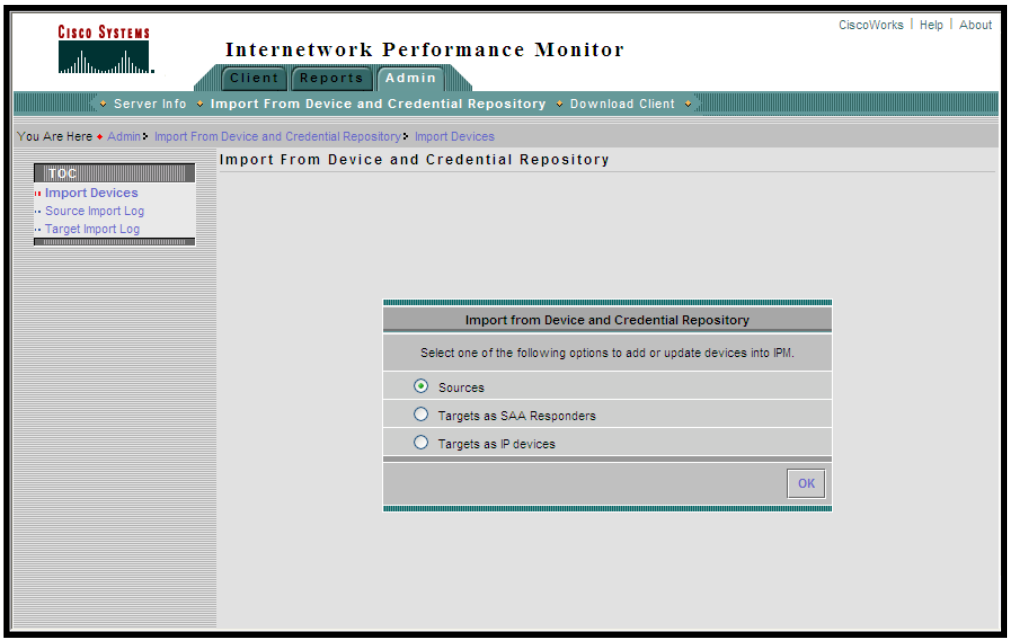


Fig: 8.32: Importando dispositivos para monitoreo dentro de Internetwork Performance Monitor.

FUENTE: Propio

Luego de presionar OK aparecerá una pantalla indicando que el proceso de importación ha terminado exitosamente, ver figura siguiente. Si se desea ver el registro de importación lo podemos hacer accediendo a ***Source Import Log*** que aparece en la figura 8.32. en su parte izquierda.

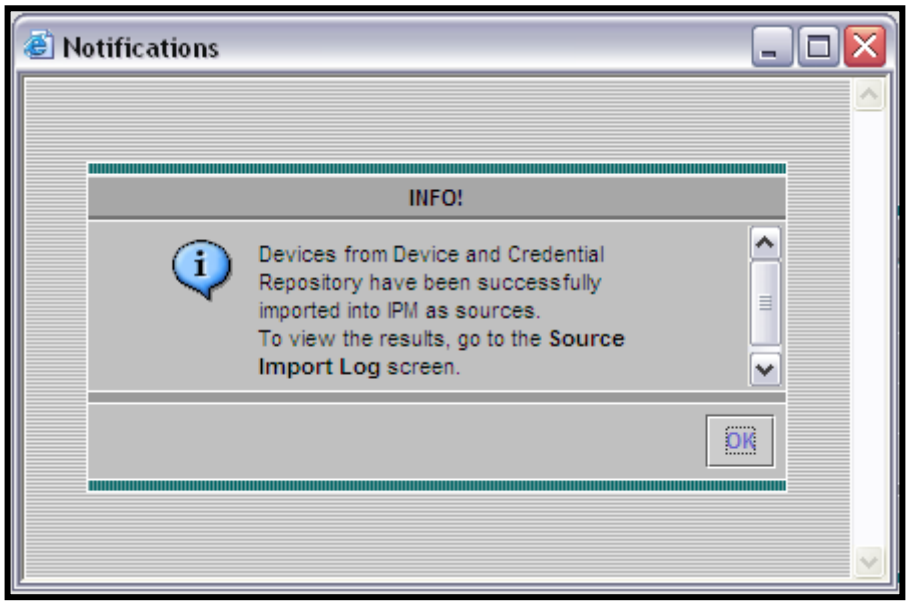


Fig: 8.33: Diálogo de confirmación de importación de dispositivos a monitorear.

FUENTE: Propio

8.6. VERIFICACIÓN DE RESULTADOS DE ADMINISTRACIÓN DE RED MEDIANTE MONITOREO DE RECURSOS EN LA RED DE PETROINDUSTRIAL.

Para monitorear uno varios dispositivos con CiscoWorks procedemos de la siguiente forma:

8.6.1. Configuración de monitoreo

Accedemos hasta Internetwork Performance Monitor > Client > Web Client; luego elegimos Edit > Configuration para hacer aparecer un nuevo menú donde se especifica los parámetros del monitoreo.

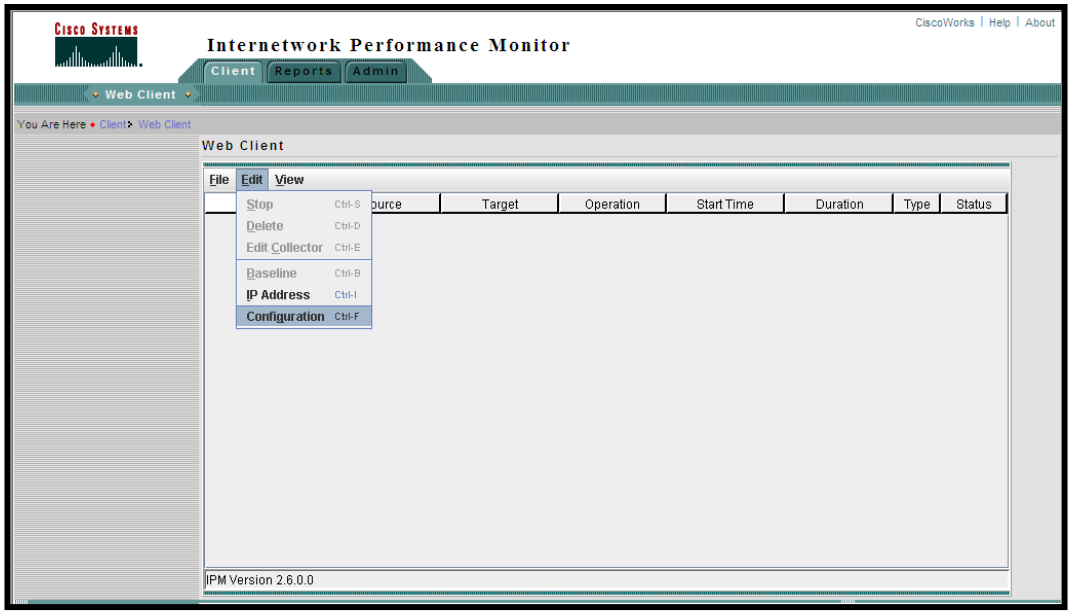


Fig: 8.34: Pantalla de Configuración de Internetwork Performance Monitor

FUENTE: Propio

En la siguiente pantalla se debe especificar nuevamente y confirmar las comunidades de lectura y escritura de SNMP para poder seguir con el monitoreo del equipo.

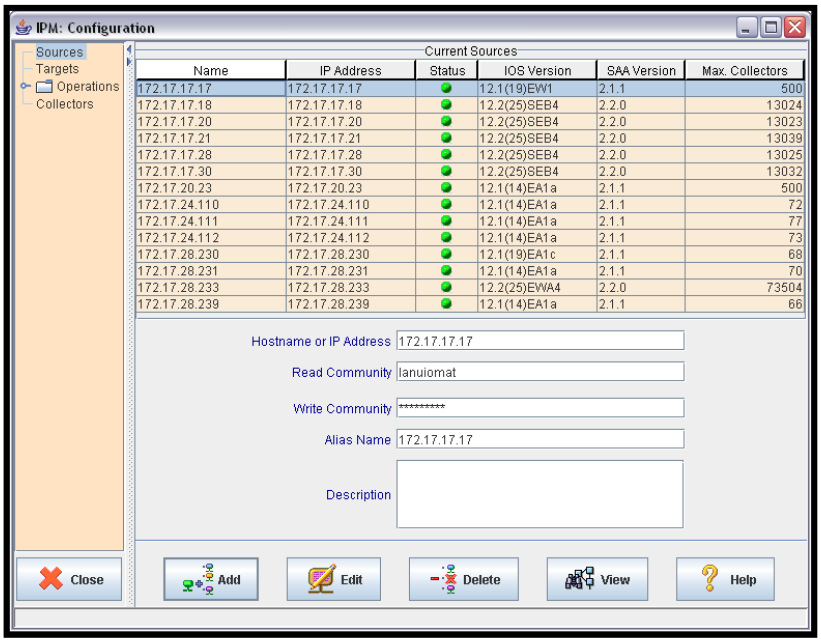


Fig: 8.35: Configuración de Datos para monitoreo de dispositivos

FUENTE: Propio

Para realizar el monitoreo de un dispositivo de la red, se debe crear un colector de información y además se debe habilitar dentro del equipo activo de red el envío de paquetes de estado para que se pueda evaluar su desempeño y generar los reportes que servirán para la corrección de errores y solución de fallas dentro de la red.

Terminado el ingreso de las comunidades y la verificación de parámetros d monitoreo, se accede a los reportes los cuales tendrán los resultados del monitoreo que se ha programado para el equipo. Así lo muestra la figura 8-35, donde se presenta el monitoreo en directo del equipo y su funcionamiento.

Las siguientes son configuraciones SNMP que deben estar habilitadas dentro de los equipos a monitorear.

Router>enable
Router#configure terminal
Router(config)#snmp-server community LANUIO ro
Router(config)#snmp-server community LANUIOCFG rw
Router(config)#snmp-server enable traps rtr
Router(config)#snmp-server host 172.17.*.* rtr
Router(config)#exit
Router#

Se puede ver estadísticas de paquetes enviados, recibidos, errores, utilización del CPU y de sus recursos principales. De la misma forma se puede habilitar el monitoreo de protocolos específicos

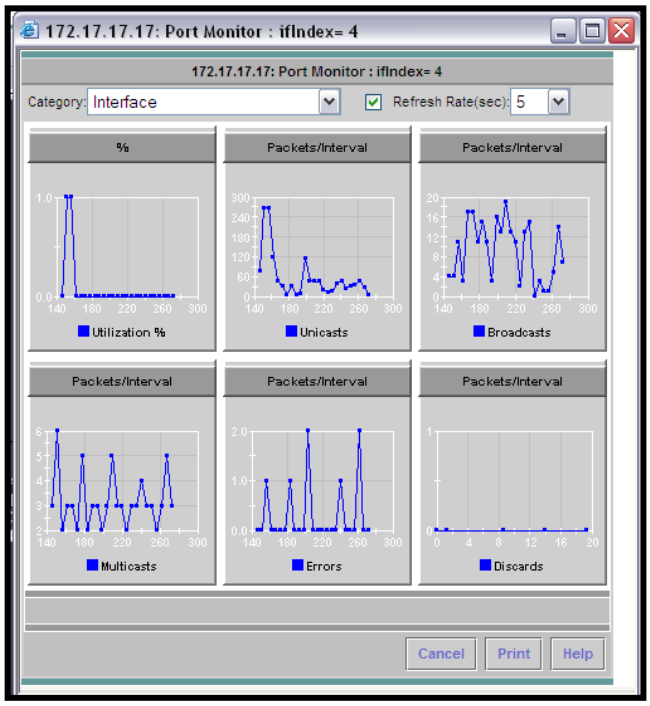


Fig: 8.36: Resultado Gráfico de Monitoreo en línea sobre una interface de un dispositivo de red.

FUENTE: Propio

De esta forma se puede mejorar evaluar el desempeño de un equipo activo de red lográndose encontrar las fuentes donde se originan los cuellos de botella o consumo excesivo de recursos de una red.

CAPITULO IX

CONCLUSIONES Y RECOMENDACIONES

9.1. Verificación de hipótesis

9.2. Conclusiones

9.3. recomendaciones

9.4. Posibles temas de tesis

9. CONCLUSIONES Y RECOMENDACIONES

9.1.VERIFICACIÓN DE HIPÓTESIS.

Con un correcto reglamento y conjunto de normas definido para administrar una Red LAN Y WAN y aplicado dentro de una herramienta como CiscoWorks, se mejora de forma notable el rendimiento y performance de la red de Petroindustrial; siempre y cuando su aplicación sea apropiada y acorde a las necesidades de crecimiento de la red y su estructura.

9.2.CONCLUSIONES.

Para lograr que un sistema de administración y monitoreo para redes LAN y WAN funcione según lo esperado se deben seguir las recomendaciones de configuración y operación del fabricante, ya que sin duda, a pesar de existir muchos tipos de herramientas para este propósito, es mejor utilizar la que recomienda el fabricante de dispositivos, pues esta podrá acceder a configuraciones propias de los equipos que las otras herramientas por su característica basadas en protocolos establecidos no podrán.

El utilizar una herramienta de administración de un fabricante de dispositivos, no permite integrar a su conjunto de equipos administrables, dispositivos de otros fabricantes, los cuales a pesar de operar con estándares internacionales no son reconocidos por dichas herramientas; y si lo hacen únicamente son mostrados como equipos existentes dentro de la red pero no se puede hacer ningún trabajo sobre ellos.

A su vez si se utiliza una herramienta general de administración, se podrá acceder a la mayoría de dispositivos activos de una red y realizar cambios sobre su configuración, pero en cambio se verán restringidas configuraciones propias y específicas que si aparecen en las herramientas del propio vendedor.

Si se desea poder mantener un estándar de administración sobre todos los equipos, es necesario estandarizar las marcas de los dispositivos, a fin de poder tener una única herramienta que permita su completa administración y monitoreo. El aspecto negativo de la estandarización, es que las empresas de hoy en día por su crecimiento, en muchos casos sin control, integran dentro de sus equipos y dispositivos múltiples marcas, muchas veces influenciado por el aspecto económico. Hay que tomar en cuenta que el estandarizar marcas tiene un elevado costo que en muchos casos no es visto como una inversión, sino como un gasto dentro de la empresa.

9.3.RECOMENDACIONES.

El instalar una herramienta para administrar equipos activos de red, no solo involucra el poseer la herramienta, sino también de la información y soporte técnico por parte del fabricante o su representante, a fin de resolver inquietudes y preguntas que surgen frecuentemente con la utilización de la herramienta.

Además se debe establecer el personal responsable que se dedique únicamente a la tarea de administrar los equipos activos de red, especialmente cuando la estructura organizacional de la empresa es tan grande y abarca una gran cantidad de equipos con múltiples tipos de configuración y fines de operación.

La capacitación del personal no solo debe enfocarse en facilitar libros o manuales acerca de una herramienta, sino también en permitir el intercambio de experiencias con otros administradores o consultores de red, a fin de encontrar un equilibrio y el mejor camino para optimizar el desempeño de una estructura tecnológica como en este caso.

El enfoque que se debe dar al área de administración de redes es primordial y estar dirigido a mejorar constantemente el desempeño tanto de la infraestructura tecnológica, como del personal que opera en esta área, ya que el mismo debe estar en la capacidad de solventar desde pequeñas fallas hasta el reemplazo completo de un equipo en el menor tiempo posible, afectando en lo mínimo a la operatividad de la empresa.

9.4.POSIBLES TEMAS DE TESIS.

Dentro de los temas de tesis que se puede proponer apegado al área de redes describo las siguientes:

- ✓ Servicios de seguridad y autenticación biométrica para redes.
- ✓ Seguridad para redes wireless sobre servidores LINUX.
- ✓ Desarrollo de herramientas de monitoreo, análisis de patrones de acceso y detección de intrusos en servidores Linux
- ✓ Desarrollo de un sistema web para monitoreo de redes y equipos de networking utilizando MRTG.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS:

1. J. García Tomás. Redes de Alta Velocidad. RAMA, 1997
2. W. Stallings. High Speed Networks. Prentice Hall 1998
3. P. Brittan and Adrian Farrel. MPLS Virtual Private Networks.
4. Catherine Paquet, Diane Teare: CCNP Self-Study: Building Scalable Cisco Internetworks (BSCI), CISCO PRESS, 201 West 103rd Street Indianapolis, IN 46290 USA. ISBN: 1-58705-084-6 April 2003.
5. Sam Halabi, Dani McPherson, Internet Routing Architectures, Second Edition, CISCO PRESS, 201 West 103rd Street Indianapolis, IN 46290 USA. ISBN: 1-57870-233-X, April 2001
6. Cisco Networking Academy Program; IT Essentials I, PC Hardware and Software Companion Guide. CISCO PRESS, 201 West 103rd Street Indianapolis, IN 46290 USA. ISBN: 1-58713-092-0. March 2003.
7. Cisco Networking Academy Program; Fundamentals of Voice and Data Cabling Companion Guide. CISCO PRESS, 201 West 103rd Street Indianapolis, IN 46290 USA. ISBN: 1-58713-087-4. June 2003
8. Cisco Networking Academy Program; IT Essentials II: Network Operating Systems Companion Guide, CISCO PRESS, 201 West 103rd Street Indianapolis, IN 46290 USA. ISBN: 1-58713-097-1, March 2003.
9. [6] Interconecting Cisco Network Devices, Vol.1 version 2.3 Student Guide ICND Version.2.3; Año 2006 Cisco Systems, Inc.
10. [29] CiscoWorks Common Services v3.0 Tutorial Cisco Systems, Inc 2005
11. [30] Implementing CiscoWorks LMS Vol.1 versión 2.5 CWENT v2.5; 2005 Cisco Systems, Inc.
12. [31] CiscoView v6.1 Tutorial Cisco Systems, Inc 2005
13. [32] Resource Manager Essentials RME v4.0 Tutorial Cisco Systems, Inc 2005
14. [33] Campus v4.0 Tutorial Cisco Systems, Inc 2005
15. [34] Device Fault Manager DFM v2.0 Tutorial Cisco Systems, Inc 2005
16. [35] Internetwork Performance Monitor IPM v2.6 Tutorial Cisco Systems, Inc 2005

REVISTAS:

1. Informativo de la Gerencia de Economía y Finanzas de Petroecuador, Año 2002 No. 017
2. [28] Manual de Procedimientos y Funciones – Petroindustrial. Año 2005

RFC's:

1. http://www.rfc-es.org/descargas.php
2. http://www.rfc-archive.org/getrfc.php?rfc=3070
3. http://www.faqs.org/rfcs/
4. ftp://ftp.isi.edu/in-notes/rfc2090.txt
5. http://www.ietf.org/rfc/rfc3277.txt
6. http://www.ietf.org/rfc/rfc1195.txt
7. http://wwwsnmp.cs.utwente.nl/ietf/rfcs/rfcbynumber.html

URL's:

1. [1] Tutorial y descripción técnica de TCP/IP: http://ditec.um.es/laso/docs/tut-tcpip/3376c11.html. 2000-07-14
2. [2] Marzo Lázaro, José Luis. "Control de Tráfico en Redes de Altas Prestaciones": http://eia.udg.es/~marzo/doctorat/ctav_v00.pdf. Año 2001.
3. [3] Goitia, María Julieta. "Protocolos de Enrutamiento para la Capa de Red en Arquitecturas de Redes de Datos": http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/ProtocolosRed.PDF. Año 2002.
4. [4] Muratori, Uzuri. "Tipos de Protocolos de Enrutamiento": http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-TiposRouting.pdf. Año 2002.
5. [5] TCP/IP Tutorial and Technical Overview: http://ditec.um.es/laso/docs/tut-tcpip/3376c33.html#vda. 2005-10-12.
6. [7] Routing Basics. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm. 2006-10-12.
7. [8] Muratori, Uzuri. "Características del Enrutamiento Dinámico en Internet": http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-Routing.pdf. Año 2005.
8. [9] Marzo Lázaro, José Luis. "Evolución de las Tecnologías y Control de Tráfico": http://eia.udg.es/~marzo/doctorat/1_doctorat_control_trafic.pdf; Año 2005; Pág. 12.
9. [10] TCP/IP Tutorial and Technical Overview: http://ditec.um.es/laso/docs/tut-tcpip/3376c12.html#arpanet. 2000-07-14.
10. [11] Interior Gateway Routing Protocol (IGRP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm. 2006-09-13.
11. [12] Enhanced Interior Gateway Routing Protocol (EIGRP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm. 2007-02-01.
12. [13] Open Shortest Path First (OSPF). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm. 2006-09-12.
13. [14] TCP/IP Tutorial and Technical Overview. EGP: http://ditec.um.es/laso/docs/tut-tcpip/3376c34.html#erp. 2000-07-14.
14. [15] Border Gateway Protocol (BGP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm. 2006-09-12.

15. [16] IS-IS - Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/IS-IS. 2006-05-12.
16. [17] Routing Information Protocol (RIP). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm. 2006-09-12.
17. [18] Switched Multimegabit Data Service (SMDS). Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/smds.htm. 2006-09-12.
18. [19] X.25 Overview. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/x25.htm. 2006-09-13.
19. [20] Frame Relay. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm. 2006-09-12.
20. [21] Interconecting Cisco Network Devices, Vol.1 version 2.3 Student Guide ICND 2.3. Año 2006.
21. [22] Asynchronous Transfer Mode (ATM) Switching. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm. 2006-09-12.
22. [23] RDSI: Telefonía y Servicios Digitales: http://www.consulintel.es/Html/Tutoriales/Articulos/rdsi.html. 2001-11-10.
23. [24] Frame Relay: 1er estándard internacional que funciona: http://www.consulintel.es/Html/Tutoriales/Articulos/frame_relay.html. 2001-11-10.
24. [25] Gigabit Ethernet. Cisco Documentation: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm. 2006-09-12.
25. [26] ATM. Tutorial y descripción técnica TCP/IP: http://ditec.um.es/laso/docs/tut-tcpip/3376c213.html#atm. 2000-07-14.
26. [27] SITE OFICIAL PETROINDUSTRIAL: http://www.petroindustrial.com.ec/frontEnd/main.php?idSeccion=7. Año 2005.
27. http://www.networksorcery.com/enp/protocol/framerelay.htm
28. http://www.dataconnection.com. Nov, 2000
29. http://www.cisco.com/warp/customer/105/48.html
30. http://www.protocols.com/pbook/frame.htm
31. http://www.arcelect.com/Frame_Relay-56kbps_FT1-T1.htm
32. http://www.wl0.org/~sjmudd/wireless/network-structure/html/index.html
33. http://eduangi.com/index.html
34. http://www.futsoft.com/pdf/fcapswp.pdf
35. http://en.wikipedia.org/wiki/FCAPS
36. http://www.cisco.com/en/US/products/sw/netmgtsw/tsd_products_support_category_home.html
37. http://www.cisco.com/en/US/products/sw/cscowork/ps2330/prod_release_note09186a00800f7dd0.html
38. http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/camp_mgr/camp_3x/cmgr_3_3/index.htm
39. http://html.rincondelvago.com/administracion-de-redes.html
40. http://www.unincca.edu.co/especial/eravd/pravd.htm
41. http://www.conocimientosweb.net/dcmt/ficha3405.html
42. http://dis.ucn.cl/Servicios/soporte_redLANWAN.htm
43. http://www.fi.upm.es/~jgarcia/
44. http://www.monografias.com/trabajos22/redes-fddi/redes-fddi.shtml

45. http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html
46. http://www.monografias.com/trabajos5/redwan/redwan.shtml
47. http://panoramix.fi.upm.es/~jgarcia/Curso_MPLS/
48. http://www.ilustrados.com/publicaciones/EpyVyypuZZCJyfYiCw.php
49. http://eia.udg.es/~marzo/doctorat/ctav_v00.pdf
50. http://www.monografias.com/trabajos/introredes/introredes.shtml
51. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm
52. http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-Routing.pdf

ANEXOS

ANEXO 1

INFORMACIÓN DETALLADA DE LAS VLAN'S CONFIGURADAS EN EL EQUIPO CISCO 4507R

1. Configuración de VTP

```
SW_CISCO_4507#show vtp status
VTP Version:                    2
Configuration Revision:         13
Maximum VLANs supported locally: 1005
Number of existing VLANs:       14
VTP Operating Mode:             Server
VTP Domain Name:                PINUIO
VTP Pruning Mode:               Enabled
VTP V2 Mode:                    Enabled
VTP Traps Generation:           Enabled
SW_CISCO_4507#
```

2. Información VLAN 1

```
interface Vlan1
description AdministracionRedes
ip address 172.17.17.17 255.255.255.192
```

3. Información VLAN 2

```
interface Vlan2
description SERVIDORES
ip address 172.17.16.19 255.255.255.0
ip helper-address 172.17.16.31
```

4. Información VLAN 3

```
interface Vlan3
```

description FINANZAS
ip address 172.17.17.65 255.255.255.192
ip helper-address 172.17.16.31
ntp broadcast

5. Información VLAN 4

interface Vlan4
description ADMINISTRACION
ip address 172.17.17.129 255.255.255.192
ip helper-address 172.17.16.31

6. Información VLAN 5

interface Vlan5
description UCC-CLOC-PASI
ip address 172.17.17.193 255.255.255.192
ip helper-address 172.17.16.31

7. Información VLAN 6

interface Vlan6
description SISTEMAS-IMP
ip address 172.17.18.1 255.255.255.192
ip helper-address 172.17.16.31

8. Información VLAN 7

interface Vlan7
description PRY-UL-CG
ip address 172.17.18.65 255.255.255.192
ip helper-address 172.17.16.31

9. Información VLAN 8

interface Vlan8
description VIC-SOP-PRD
ip address 172.17.18.129 255.255.255.192
ip helper-address 172.17.16.31

10. Información VLAN 9

```
interface Vlan9
description Telefonia
ip address 172.17.116.10 255.255.255.0
ip helper-address 172.17.16.31
```

11. Información VLAN 10

```
interface Vlan10
description Seguridad
ip address 172.17.117.10 255.255.255.0
ip helper-address 172.17.16.31
```

12. Información Default Gateway

```
ip default-gateway 172.17.16.23
```

ANEXO 2

INFORMACIÓN DE LA TABLA DE RUTAS CONFIGURADAS EN EL EQUIPO CISCO 4507R

1. Tabla de Rutas en Cisco 4507

ip route 0.0.0.0 0.0.0.0 172.17.16.23	Ruta Default Gateway
ip route 10.10.10.0 255.255.255.0 172.19.230.14	Red de Petroecuador
ip route 172.16.2.0 255.255.255.0 172.19.230.12	Red de MEM-DNH
ip route 172.16.3.0 255.255.255.0 172.19.230.12	Red de MEM-DNH
ip route 172.17.20.0 255.255.252.0 172.17.16.23	Red de Esmeraldas
ip route 172.17.24.0 255.255.252.0 172.17.16.23	Red de Shushufindi
ip route 172.17.28.0 255.255.252.0 172.17.16.23	Red de Libertad
ip route 172.17.33.0 255.255.255.0 172.17.16.23	Red LAN PIN-MATRIZ
ip route 172.19.226.0 255.255.255.0 172.17.16.23	Red de Telefonía IP

ANEXO 3

CONFIGURACIONES DE EQUIPOS RUTEADORES VANGUARD-MOTOROLA

1. ROUTER PETROINDUSTRIAL MATRIZ

```
********************************************************************************
Node: UIO_PIN   Address: 251              Date: 10-APR-2007  Time: 16:04:33
 Detailed Node Statistics                       Page:  1 of  9

Node number: 251                          Uptime: 39243 minutes
Product Type: VANGUARD 6455
Node Serial #: 141515608
PROM revision: 5.3
Code Revision: V6.4.R00A_@Rosan20a_6455 (12-Apr-05 10:44:39  Size: 4695900 bytes

Flash Revision, Current:   V6.4.R00A_@Rosan20a_645  Size: 3949676 bytes  Bank: 1
Flash Revision, Alternate: None  Bank: 2

Last power up or reset:       13-MAR-2007 12:17:23
Last manual node boot:        14-MAR-2007 12:35:39
Last watch-dog timeout event: <none>
Last configuration change:    05-APR-2007 11:57:49

Compressed config. memory (CMEM):    63488 bytes avail,   9792 bytes (15%) used
Uncompressed config. memory (SDRAM): 393216 bytes avail,  32734 bytes (8%) used
```

```
********************************************************************************
 Node: UIO_PIN   Address: 251              Date: 10-APR-2007  Time: 16:07:30
Detailed Node Statistics                        Page:  5 of  9

Motherboard:   Number of ports: 16   Status: Running
Assembly: 74347G02  Version:  K  Serial Number: 141515608

Memory Configuration:
   Total SDRAM size: 32 MBytes
   On-Board FLASH: 4 MBytes   FLASH SIMM: Not Installed

Port Configuration:
   Port  1: V.36         DTE          Port  9: NONE
   Port  2: V.36         DTE          Port 10: NONE
   Port  3: EIA-232-D    DCE          Port 11: NONE
   Port  4: EIA-232-D    DCE          Port 12: NONE
   Port  5: ETHERNET     10BASE-T     Port 13: VRDC_4FXO    PORTS 71-74
   Port  6: NONE                      Port 14: NONE
   Port  7: NONE                      Port 15: NONE
   Port  8: NONE                      Port 16: NONE

CPU Utilization Curr.: 46%, CPU Average: 54%, CPU Max: 98% 23-MAR-2007 16:02:42
```

2. ROUTER REFINERÍA ESTATAL ESMERALDAS

```
********************************************************************************
Node: ESMEPIN   Address: 630              Date: 11-APR-2007  Time:  7:59:41
 Detailed Node Statistics                       Page:  1 of  9

Node number: 630                          Uptime: 2382 minutes
Product Type: VANGUARD 6455
Node Serial #: 141515612
PROM revision: 5.3
Code Revision: V6.4.TD1H_@petcISDN_6455 (24-Jan-07 15:59:27  Size: 6518364 bytes
ISDN BRI Switch Types available: ETSI, QSIG
ISDN PRI Switch Types available: NONE
Flash Revision, Current:   V6.4.TD1H_@petcISDN_645  Size: 5250668 bytes  Bank: 1
Flash Revision, Alternate: V6.4.TD1H_@petcISDN_645  Size: 5250668 bytes  Bank: 2

Last power up or reset:       09-APR-2007 16:26:00
Last manual node boot:        28-MAR-2007 10:46:33
Last watch-dog timeout event: <none>
Last configuration change:    29-MAR-2007 08:57:46


Compressed config. memory (CMEM):   129024 bytes avail,   4036 bytes (3%) used
Uncompressed config. memory (SDRAM): 786432 bytes avail,  11774 bytes (1%) used

 Press any key to continue ( ESC to exit ) ...
```

```
********************************************************************************
Node: ESMEPIN   Address: 630              Date: 11-APR-2007  Time:  8:01:25
 Detailed Node Statistics                       Page:  5 of  9

Motherboard:   Number of ports: 16   Status: Running
Assembly: 74347G02  Version:  K  Serial Number: 141515612

Memory Configuration:
   Total SDRAM size: 32 MBytes
   On-Board FLASH: 4 MBytes   FLASH SIMM: 8 Mbytes

Port Configuration:
   Port  1: V.36         DTE          Port  9: NONE
   Port  2: V.36         DTE          Port 10: VRDC_4FXS     PORTS 61-64
   Port  3: EIA-232-D    DCE          Port 11: NONE
   Port  4: EIA-232-D    DCE          Port 12: NONE
   Port  5: ETHERNET     10BASE-T     Port 13: VRDC_4FXO     PORTS 71-74
   Port  6: NONE                      Port 14: NONE
   Port  7: VRDC_4FXS    PORTS 51-54  Port 15: NONE
   Port  8: NONE                      Port 16: NONE

CPU Utilization Curr.: 28%, CPU Average: 22%, CPU Max: 58% 10-APR-2007 07:59:34


 Press any key to continue ( ESC to exit ) ...
```

3. ROUTER REFINERÍA LA LIBERTAD

```
********************************************************************************
Node: PIN_CAB   Address: 471              Date: 11-APR-2007  Time:  7:40:04
 Detailed Node Statistics                       Page:  1 of  7

Node number: 471                          Uptime: 56051 minutes
Product Type: VANGUARD 6435
Node Serial #: 141513613
PROM revision: 5.1
Code Revision: V6.3.R00A_@IP+20_6435 (19-Jan-04 10:23:02)    Size: 4396028 bytes


Flash Revision, Current:   V6.3.R00A_@IP+20_6435    Size: 3974128 bytes  Bank: 1
Flash Revision, Alternate: None  Bank: 2

Last power up or reset:       03-MAR-2007 13:11:44
Last manual node boot:        18-SEP-2006 09:29:58
Last watch-dog timeout event: <none>
Last configuration change:    26-JAN-2007 08:37:26


Compressed config. memory (CMEM):    63488 bytes avail,   3832 bytes (6%) used
Uncompressed config. memory (SDRAM): 393216 bytes avail,   9524 bytes (2%) used

 Press any key to continue ( ESC to exit ) ...
```

```
********************************************************************************
Node: PIN_CAB   Address: 471              Date: 11-APR-2007  Time:  7:41:21
 Detailed Node Statistics                       Page:  5 of  7

Motherboard:   Number of ports: 16   Status: Running
Assembly: 74347G22  Version:  K  Serial Number: 141513613

Memory Configuration:
   Total SDRAM size: 32 MBytes
   On-Board FLASH: 4 MBytes   FLASH SIMM: Not Installed

Port Configuration:
   Port  1: V.36         DCE          Port  9: NONE
   Port  2: V.36         DTE          Port 10: TDM          E1
   Port  3: EIA-232-D    DCE          Port 11: TDM          E1
   Port  4: EIA-232-D    DCE          Port 12: TDM          E1
   Port  5: ETHERNET     10BASE-T     Port 13: NONE
   Port  6: NONE                      Port 14: NONE
   Port  7: NONE                      Port 15: NONE
   Port  8: NONE                      Port 16: NONE

CPU Utilization Curr.: 3%, CPU Average: 3%, CPU Max: 76% 09-APR-2007 11:43:06


 Press any key to continue ( ESC to exit ) ...
```

4. ROUTER COMPLEJO INDUSTRIAL SHUSHUFINDI

```
**************************************************************************
 Node: SHUSHPIN  Address: 820              Date: 11-APR-2007  Time:  7:47:54
 Detailed Node Statistics                    Page:  1 of  9

Node number: 820                          Uptime: 30151 minutes
Product Type: VANGUARD 6455
Node Serial #: 141407302
PROM revision: 5.3
Code Revision: V6.4.TD1H_@petcISDN_6455 (24-Jan-07 15:59:27  Size: 6518364 bytes
ISDN BRI Switch Types available: ETSI, QSIG
ISDN PRI Switch Types available: NONE
Flash Revision, Current:   V6.4.TD1H_@petcISDN_645  Size: 5250668 bytes  Bank: 1
Flash Revision, Alternate: V6.4.TD1H_@petcISDN_645  Size: 5250668 bytes  Bank: 2

Last power up or reset:       04-MAR-2007 17:01:14
Last manual node boot:        21-MAR-2007 11:14:51
Last watch-dog timeout event: <none>
Last configuration change:    23-MAR-2007 14:01:15


Compressed config. memory (CMEM):   129024 bytes avail,   4302 bytes (3%) used
Uncompressed config. memory (SDRAM): 786432 bytes avail,  12368 bytes (1%) used

 Press any key to continue ( ESC to exit ) ...
```

```
**************************************************************************
 Node: SHUSHPIN  Address: 820              Date: 11-APR-2007  Time:  7:48:58
 Detailed Node Statistics                    Page:  5 of  9

Motherboard:   Number of ports: 16   Status: Running
Assembly: 74347G02  Version:  J  Serial Number: 141407302

Memory Configuration:
   Total SDRAM size: 32 MBytes
   On-Board FLASH: 4 MBytes   FLASH SIMM: 8 Mbytes

Port Configuration:
   Port  1: EIA-232-D     DTE          Port  9: NONE
   Port  2: V.36          DTE          Port 10: VRDC_4FXS     PORTS 61-64
   Port  3: EIA-232-D     DCE          Port 11: NONE
   Port  4: EIA-232-D     DCE          Port 12: NONE
   Port  5: ETHERNET      10BASE-T     Port 13: NONE
   Port  6: NONE                       Port 14: NONE
   Port  7: VRDC_4FXS     PORTS 51-54  Port 15: NONE
   Port  8: NONE                       Port 16: NONE

CPU Utilization Curr.: 9%, CPU Average: 8%, CPU Max: 53% 02-APR-2007 17:41:03


 Press any key to continue ( ESC to exit ) ...
```

GLOSARIO TECNOLÓGICO

A	
AIX	AIX (Advanced Interactive eXecutive) es un sistema operativo UNIX propietario de IBM. Inicialmente significaba "Advanced IBM Unix" pero probablemente el nombre no fue aprobado por el departamento legal y fue cambiado a "Advanced Interactive eXecutive"
ARPANET	Advanced Research Projects Network
AS	Autonomous System ó Sistema Autónomo
ATM	Asynchronous Transfer Mode ó Modo de Transferencia Asincrónico
AVVID	AVVID, es la arquitectura para voz, video y datos integrados, permiten a las empresas extender el valor de sus redes. Cisco AVVID entrega una óptima calidad en el servicio, en la seguridad y en la disponibilidad de la red, dando una base sólida para el desarrollo rápido de los servicios y aplicaciones integrado.
B	
BackBone	Bus que se puede utilizar para interconectar maquinas o LAN's entre diferentes pisos o diferentes edificios (Vertical u Horizontal), puede ser un bus o un anillo, debe de ser de mayor velocidad de la que este manejando alguna de las LAN's que va a interconectar
Banda Ancha	Transmite múltiples señales de portadora de alta frecuencia, emplea FDM. Envía señales de forma simultánea. Maneja múltiples canales de diferentes velocidades, no necesita ser digitalizada las señales.
Banda Base	Transmisión Digital de una señal, la transmisión se realiza una a la vez. Utiliza TDM, puede enviar voz datos pero siempre y cuando sean digitalizados, es barata.
Baudio	Unidad que se utiliza para las velocidades de los Modem's. Se refiere al cambio de un nivel (alto) a otro (bajo), en el envío de información al momento de un transmisión. Esta referido a la Transmisión y la Recepción de tramas
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BIS	Border Intermediate Systems
Bit	Símbolo que se propaga en el canal de información en un determinado tiempo (referido al canal de información). Unidad más pequeña de información.
Bridge	En español Puente. Se utiliza para conectar dos redes que sean diferentes en su capa de Enlace de Datos
Broadcast	Envió de información a múltiples destinos que son desconocidos para el transmisor. Normalmente utilizado por los Router para reconocimientos de Host
Brouter	Unión de un Bridge y un Router. Dispositivo de red que funciona como enrutador para el envío de datos a una red de destinos y como un Bridge para conectar dos redes entre sí.

Buffer	Dispositivo que se utiliza como memoria de paso, solo deja salir la información cuando se le indica y recibe información una vez que esta vació. Se puede utilizar como protección para diferentes etapas.
C	
CAD	Diseño Asistido por Computadora. Regularmente son terminales de control numérico que pueden estar conectadas a la red.
CCITT	Comité Consultivo Internacional para Telegrafía y Telefonía
CCO	Cisco Connection Online
CDP	Cisco Discovery Protocol
CIDR	Classless Interdomain Routing
Colisión	Es aquella que sucedes cuando 2 o más tramas que se estén enviando por un medio de transmisión coincidan y choquen entre ellas y esto haga que las tramas se fracturen y por lo tanto el destino no pueda reconocer la información y por lo tanto se pierda
CPE	Customer Premises Equipment
CSMA/CD	En ingles Carrier Sense Múltiple Access / Colision Detect. Acceso Múltiple por Detección de Portadora / Detección de Colisiones. Utilizado por Ethernet para la detección de colisiones y está ubicado en la subcapa MAC del modelo OSI
D	
DCE	Data Circuit-Terminating Equipment
DEC	Digital Equipment Corporation
DFM	Device Fault Manager
DLCI	data-link connection identifiers
DNS	En ingles Domain Name System. Nombre del Dominio del Sistema. Este establece una correspondencia entre la dirección IP con un dominio.
DQDB	Distributed Queue Dual Bus
DSL	Digital Subscriber Line
DTE	Data Terminal Equipment
Dúplex	En ingles Full Dúplex Es la forma de comunicación de un sistema. Este puede transmitir información en ambos sentidos y puede transmitir y recibir información al mismo tiempo
E	
EBGP	Exterior Border Gateway Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol

ETCD	En ingles DCE. Equipo Terminal de Circuito de Datos. Es la interfaz de un ETD.
ETD	Equipo Terminal de Datos. Conocida también como equipo final, donde llega la información o se transmite la información.
Ethernet	Ether- Eter, Net- Red Red de Eter. Es el nombre que se le dio a la Red debido a su similitud que tiene con todo en el universo, ya que esta red es un universo de información.
F	
FCC	Comisión Federal de Comunicaciones
FCS	En ingles Frame Check Secuence. Esta se utiliza para la detección de errores al momento de enviar información. Se encuentra dentro del Trailer de la trama. Es parte del CRC
FDDI	En ingles Fiber Distribution Data Interface. Permite integrar otro tipo de redes, utilizando anillos de Fibra Óptica. Emplea Estaciones DAS y SAS. Sus enlaces entere las interfaz es de hasta 2 Km.
FECN	Forward Explicit Congestion Notification
Frame	Bloque de datos en una transmisión por tarjeta de red, se le conoce como trama (es el formato de un paquete). También se aplica para describir el Formato de una página de Internet
Front End	Es un ETCD. Este se encarga de controlar y conmutar a las diferentes terminales, este maneja diferentes velocidades de transmisión.
FTP	En ingles File Transfer Protocol. Protocolo de Transferencia de Archivos. Este es el que nos permite transferir archivos en internet, a demás de copiarlos y poder distinguir entre dos tipos de archivos que pueden ser binarios o ASCII.
FXO	Foreign Exchange Office, es un dispositivo de computador que permite conectar éste a la Red Telefónica Conmutada, y mediante un software especial, realizar y recibir llamadas de teléfono.
FXS	Foreign Exchange Station sirven para conectar teléfonos analógicos normales a un computador, y mediante un software especial, realizar y recibir llamadas hacia el exterior, o hacia otros interfaces FXS.
G	
Gateway	En español Pasarela. Es una dirección que se tiene en el ruteador (Router) puede ser interior o exterior.
GBIC	Gigabit Interface Converter, Convertidores de Interfaz Gigabit, es un transmisor-receptor que convierte las señales eléctricas utilizado entre los adaptadores del transportador anfitrión (dispositivos similares del canal y de Ethernet de fibra) y las señales eléctricas u ópticas convenientes para la transmisión. Los convertidores de interfaz del gigabit, permiten que los diseñadores obtengan un tipo de dispositivo y que lo adapten para el cobre u otros usos ópticos.
H	
HDTV	Televisión de Alta Definición

HP-UX	HP-UX es la versión de Unix de Hewlett-Packard. HP-UX es la versión de Unix desarrollada y mantenida por Hewlett-Packard desde 1983
I	
IBGP	Interior Border Gateway Protocolo
ICMP	En ingles Internet Control Message Protocol. Envía mensajes de error cuando IP, no puede encaminar a la información.
IDRP	Interdomain Routing Protocol
IEEE	The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización,
IETF	Internet Engineering Task Force
IETF	Internet Engineering Task Force
IGMP	En ingles Internet Group Management Protocol. Administra a los grupos de Host que pertenezcan a una red de área local
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
Interfaz	En ingles Interface. Que significa entre caras, es un acoplamiento mecánico
Inundación	Ataque de denegación de servicios donde el ordenador es atacado con mensajes. Algoritmos de enrutamiento o Flooding (Algoritmo de enrutamiento), no adaptivo, utilizado para el enrutamiento de los datos guardados en paquetes.
IOS	Internetwork Operating System
IP	En ingles Internet Protocol. Protocolo de internet, es el que se encarga del encaminamiento y selección de las rutas. Se encuentra en la capa de red del modelo OSI.
IPM	Internetwork Performance Monitor
IPX	IPX/SPX, Internetwork Packet Exchange/Sequenced Packet Exchange (Intercambio de paquetes interred/Intercambio de paquetes secuenciales), es un protocolo de red utilizado por los sistemas operativos Novell Netware
ISDN	Integrated Services Digital Network, conocido también como Red Digital de Servicios Integrados
IS-IS	Intermediate System-to-Intermediate System
ISO/CLNP	International Organization for standardization/Connectionless Network Protocol
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
L	
LAN	En ingles Local Area Network. Red de Area Local, es un conjunto de computadoras las cuales pueden estar conectadas en diferentes formas

	(topologías)
LAPB	Link Access Procedure, Balanced
LLC	En ingles Logic Link Control. Control de Enlace Lógico, es el procedimiento de enlace entre dos maquinas de forma lógica para no confundir la transmisión.
LMS	LAN Management Solution
LSA	Anuncio de Estado de Enlace
M	
MAC	En ingles Médium Access Control. Control de Acceso al Medio. Son las reglas que se utilizan para normar la forma de cómo los nodos van a funcionar, es la que va a determinar que maquina va a tener prioridad.
MAN	red de área metropolitana (Metropolitan Area Network o MAN, en inglés) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa
Medio Dúplex	Half Dúplex. La comunicación es en dos sentidos con la característica de que solo puede transmitir o recibir información en tiempos distintos.
MIB	En ingles Management Information Base. Administración de la Base de Información. Es la que se encarga de administrar la información del SNMP.
Modem	Combinación de Mod- Modulador y Dem- Demodulador. Dispositivo de Interfaz de un ETD para la Conexión a internet.
Multicast	Envío de información a múltiples destinos conocidos. Esto se utiliza en las direcciones de Clase D de IP.
N	
NGI	Internet de la Próxima Generación
NOS	En ingles Network Operate System. Sistema Operativo de Red, es el que se tiene en una red de área local.
NSM	Network Management System
O	
OSI	En ingles Open System Interconection. Interconexión de Sistemas Abiertos. Este se utiliza para la conexión de equipos que no son de una misma fábrica. Está constituido por 7 Capas: Físico, Enlace de Datos, Red, Transporte, Sesión Presentación Aplicación.
OSPF	Open Shortest Path First Protocolo de encaminamiento, localizado en el NOS, toma la decisión en función del camino más corto. Tiene menos saltos (La ruta tiene menor número de ruteadores).
P	

PABX	Sistema Electrónico de Conmutación
PAD	Packet Assembler/Disassembler
Paquete	Es un Bloque de Datos, una trama
PBX	PBX es el acrónimo de Private Branch eXchange o Private Business eXchange, Centrales Telefónicas empresariales
PDN	Public Data Networks
PDU	En ingles Protocol Data Unit. Unidad de datos del Protocolo, es una unidad de datos que se forma en el protocolo de nivel de enlace de datos (MAC), un datagrama es un PDU.
PLC	Se utilizan para accesos automáticos, también controlan datos.
PLCP	Physical Layer Convergency Protocol
PLP	Packet Layer Protocol
PPP	En ingles Point to Point Protocol. Protocolo Punto a Punto, se utiliza para realizar una conexión de un PC directamente a internet.
Protocolo	Conjunto de reglas necesarias para poder establecer una comunicación entre dos ETD y así intercambiar información.
Proxy	Se utiliza para mandar y recibir datagramas en red, también se usa para conectar a internet y esta a su vez le proporcione la conexión de internet a las otras Host.
PSE	Packet-Switching Exchange
PSN	Packet-Switched Networks
PVC	Permanent Virtual Circuits
R	
RAID	Componente que se inserta en el Sistema Operativo. Para buscar los mensajes de un buzón que puede estar en varios discos duros o en diferentes partes de un disco duro.
RARP	En ingles Reverse Addres Resolution Protocol. Este hace una relación de la dirección de la tarjeta de red (Física) y la dirección IP. Hace la función inversa de ARP.
RCP	Remote Copy Protocol
Red	Interconexión de Nodos a través de medios de transmisión alámbricos o inalámbricos
Red Orientada a Conexión	Aquella que tiene conexión virtuales o lógicas (circuitos virtuales), tipo WAN, Internet, MAN
Red sin Conexión	Este tipo de red utiliza datagramas
Repetidor Multipuerto	Un repetidor es la expresión mínima de un concentrador, o también se puede decir, que un concentrador es un repetidor multipuerto.
RFC	En ingles Revest For Coustomer. Maneja los documentos de internet como UDP, IP, ICMP,SMTP, FTP,etc.
RIP	Routing Information Protocol. Protocolo de encaminamiento, localizado en el NOS, toma la decisión en función del camino más corto, tiene menos saltos (la ruta tiene menor número de ruteadores).

RME	Resource Manager Essentials
Router	Dispositivo de la red utilizado para conectar dos redes de área local con diferentes capas de Red.
Ruta de Default	Es la que se toma cotidianamente, no necesariamente es la más corta.
RWAN	Routed WAN Management Solution
S	
SAS	En ingles Simple Attachment Sattion. Se utiliza para conectar directamente a los nodos en el anillo del FDDI
SDH	Synchronous Digital Hierarchy
SDU	Unidades de Datos SMDS
Simplex	Comunicación de sistemas en un solo sentido. El envió de información es de un ETD origen a un ETD destino.
SIN	Subscriber Network Interface
SIP	SMDS Interface Protocol
SLA	Acuerdos de Nivel de Servicio (SLAs
SMDS	Switched Multimegabit Data Service
SMS	Service Management Solution
SMTP	En ingles Simple Mail Transfer Protocol. Utiliza a DNS para luego DNS apoyarse de TCP. Esto lo hace con el objetivo de enlazar a IP con TCP y así poder administrar a los correos electrónicos.
SNMP	En ingles Simple Network Management Protocol. Usa los servicios de UDP, se utiliza para tener un control de las Host, asignando a una terminal como administrador la cual por medio de una base de datos llamada MIB actualizando la información de que paginas a visitada o acciones ha realizado de cada uno de los agentes (host).
SONET	Synchronous Optical Network
SPF	Algoritmo de Shortest Path First ó primero el camino más corto
Split Horizons	Horizonte Dividido
Store/Forward	Almacena y envía las tramas que se tienen en la red.
SVC	Switched Virtual Circuits
Switch	El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. El switch funciona una capa más arriba y es más inteligente que el hub.
T	
Tablas de Ruteo	Contiene las direcciones de las interfaz, las host y a demás las rutas.
TCP	En ingles Transmisión Control Protocol. Interfaz entre las aplicaciones y la dirección IP. Localizado en la capa de enlace del

	modelo OSI.
Terminal	Es una ETD, procesan y almacenan información.
TFTP	Trivial File Transfer Protocol
Throughput	Rendimiento de procesamiento
Token	Es conocido como Ficha o Testigo. Es una trama pequeña que no tiene datos de usuario, solo tiene Header y Trailer. Este es usado en Token Ring y Token Bus.
Topología	Forma geométrica que adquiere la red al conectarse las terminales con los enlaces.
TOS	Type-of-Service
Trafico Asíncrono	Este tipo de tráfico es muy sensible al retardo debido a su falta de sincronía.
Trafico Síncrono	Este se maneja en tiempo real y no sufre de ningún retardo de información.
Trailer	Termino que se le da a la parte inferior de una trama de datos, también conocido como cola y consta de un delimitador y un campo de control que lleva el código de detección de errores.
TTL	En ingles Time to Life. Tiempo de Vida media que el datagrama puede sobrevivir en la red, antes de ser desechada la trama.
U	
UDP	En ingles User Data Protocol. Protocolo de uso de datos, este se encuentra en la misma capa de TCP y se utiliza para ligar algunas aplicaciones.
URL	En ingles Universal Resource Identificator. Este es la forma como se identifican los diferentes servidores o direcciones de Internet.
V	
VMS	VPN/Security Management Solution
VPN	Virtual Private Network ó Redes Privadas Virtuales
VTP	VTP son las siglas de VLAN Trunking Protocol, un protocolo usado para configurar y administrar VLANs en equipos Cisco.
W	
WAN	En Ingles Wide Area Network. Red de Área Amplia, esta es de un rango mayor a las redes de área local.
X	
X.25	Es un estándar UIT-T para redes de área amplia de conmutación de paquetes
XNS	Xerox Network System