SEP **SNEST** **DEGEST**

INSTITUTO TECNOLÓGICO DE TUXTLA GUTIÉRREZ

"SEGMENTACIÓN DE LA RED DE DATOS DEL SECTOR DE TRASMISIÓN CHICOASEN MEDIANTE LA CREACIÓN DE VLAN'S"

MEMORIA DE RESIDENCIA PROFESIONAL

PRESENTA:

NOMBRE: REYES GONZÁLEZ JOSÉ ALFONSO

N. CONTROL: 07270340

ASESOR INTERNO ITTG:

ING. GERARDO FERNANDO DÍAZ BORREGO

ASESOR EXTERNO CFE:

ENRIQUE ALONSO MÉNDEZ JIMÉNEZ

ING. ELECTRÓNICA

ÍNDICE

3. METODOLOGÍA

4. ANÁLISIS DE RESULTADOS

ANEXOS

CONCLUSIONES

REFERENCIA BIBLIOGRAFÍA Y VIRTUAL

RESUMEN

Este documento nos presenta un proyecto que consiste en el diseño de una segmentación de red por medio de redes virtuales (VLAN's) utilizando la red LAN que actualmente está en uso en el sector de transmisión Chicoasen ,esto con el objetivo de administrar y eficientar el ancho de banda de la red de datos por aplicaciones y procesos, la optimización implica que como red se cubran las características más importantes que una red de datos requiere las cuales son : la tolerancia a fallas, escalabilidad, calidad de servicio y seguridad, esto se ara sobre la LAN que actualmente existe haciéndole modificaciones a nivel software y hardware ya que para que las VLAN'S creadas lleven a cabo su propósito y sea bien complementado se agregaran actualizaciones físicas y un sistema de seguridad por medio de equipos firewall.

Así, realizando los cambios pertinentes tendremos entonces un entorno más eficiente y seguro con todos los beneficios que una segmentación bien elaborada nos proporciona beneficiando así directamente a usuarios de equipos informáticos y equipos dedicados.

PALABRAS CLAVE:

RED DE DATOS, LAN, MAN, WAN, SWITCH, ROUTER, SEGMENTACIÓN, FIREWALL, CABLEADO ESTRUCTURADO, INTERNET, INTRANET. ETHERNET, TCP/IP.

1. INTRODUCCIÓN

A lo largo de la historia la comunicación del ser humano se ha ido desarrollando y evolucionando de manera abrupta adaptándose paralelamente al crecimiento de la población y el desarrollo humano, haciendo así cada vez más necesarios los medios inventiva del hombre para poder satisfacer las necesidades que actualmente se presentan, estos cambios en el siglo pasado y en el presente evolucionaron volviéndose así área de estudio constante.

CFE es consiente que por su estructura en cuanto el gran número de personal, y su gran cantidad de equipos requiere del desarrollo constante de diseños apoyados de equipos de tecnología de punta para que esta empresa que satisface la necesidad de un país entero logre su fin en base a las normas de calidad más altas.

El Sector de Transmisión Chicoasen es parte muy importante de la empresa y por lo tanto cuenta con una red de datos de gran envergadura , sin embargo en base a lo ya dicho , se contempló hacer una modificación y actualización adecuada a la necesidad que se presenta en cada departamento que convive dentro de la LAN, para ello cada diseño desarrollado que se elaboró en cuanto a administración y funcionamiento se hizo en base a un estudio minucioso el cual fue en base a recopilación de datos anualizando cada necesidad en la red.

La segmentación de la Red mediante la creación de VLAN´S bien pudo haberse limitado a la programación del switch principal 3750 CISCO que brinda el servicio a cada eslabón de la red por medio de un enlace , pero ya que CFE cuenta con los medios y nace la necesidad de profundizar más en el proceso, se ha hecho una nueva distribución de cableado donde se requirió, y se implementó un cableado estructurado en cierto segmento físico y virtual de la red, además de un sistema redúndate de protección por medio de equipos firewall.

Este tipo de cambios realizados resultan de un costo elevado pero son necesarios y su fin justifica el alto precio que ello conlleva , CFE es una empresa de clase mundial y su servicio debe ser análogo a lo que su imagen representa por tanto cualquier modificación que se allá echo a la red de datos y que es presentada en este documento puede que en un plazo no muy largo sea de nuevo reconfigurada siempre con el fin de dar un mejor servicio al personal de la empresa y equipos dedicados pero sobre todos al usuario final del servicio que CFE proporciona.

1.1 JUSTIFICACIÓN DEL PROYECTO

El proyecto de "Segmentación de red de datos del Sector de Transmisión Chicoasen mediante la creación de VLAN's es elaborado con el fin de alcanzar objetivos bien establecidos, partiendo por el hecho de que el hacerlo va de la mano la restructuración física de la red, la cual es necesaria ya que no se cuenta con un sistema estandarizado el cual nos permita un transporte de datos fiable y robusto como lo requieren tantos usuarios, aplicaciones, servicios , principalmente los equipos del departamento de Control y el de Protección y Mediciones los cuales deben estar protegidos de manera estricta.

El hacer esta innovación y estos cambios en la red nos da como resultado también una optimización y mejor desempeño de equipos dedicados al monitoreo y operación en una subestación ya que se evitara que en su alojamiento, la caseta de control principal ocurran interferencia electromagnéticas IEMI en la red de comunicaciones lo cual sucede muy a menudo.

Reestructurar la red física y proteger mediante equipos firewalls, y a segmentar por medio de VLAN's trae consigo las siguientes mejoras las cuales son indispensables:

- Aumento de velocidad en el ancho de banda para los equipos que lo requiere ya que el cableado estructurado y la programación adecuada en las VLAN nos permite asignar velocidades mucho más altas de lo que es normalmente en una red convencional y el cableado da oportunidad de operaciones más robustas, así como evitar errores en la transmisión por broadcast.
- Seguridad en cada puerto ya que se separan usuarios y se evita la invasión de intrusos no autorizados en algún segmento de red sin previa configuración al switch principal el cual solo permite convivencia entre puertos y segmentos de acuerdo a la programación que se prestablece.
- Un aumento considerable en la seguridad muy necesario con respecto a la red interna del Control Supervisorío y Protecciones y Mediciones en las que se necesitan niveles de seguridad muy altos
- Menor riesgo en mantenimiento a los equipos del departamento de control y protecciones puesto que se canalizan los cableados por una misma escalerilla, donde es muy necesario para tener orden en espacio demasiado reducidos.
- Diagramas establecidos que permiten actuar más rápida y eficientemente al introducir nuevos equipos y usuarios en la red de datos y dar soluciones a problemas que surgen dentro de la red.
- Un panorama más claro para una segmentación futura a niveles más altos en el cual se desea aplicar nuevas modificaciones físicas o trabajar abiertamente con diversos protocolos disponibles.

1.2 OBJETIVOS

1.2.1 OBJETIVOS GENERALES

Administrar y eficientar la red de datos con la creación de VLAN'S, acompañada de procesos de cambio a programación de equipos que lo requieren, instalación de cableado estructurado, y puestas en servicio de equipos de seguridad firewall.

1.2.2 OBJETIVOS ESPECÍFICOS

- Lograr un sistema de seguridad; para evitar acceso a personas no autorizadas tanto internas como externas por medio de las VLAN's.
- Reasignación de direcciones IP a cada usuario; para una buena identificación de quien recibe el servicio y ver en que VLAN puede ubicarse.
- Reasignación de ancho de banda para que usuarios o equipos que requieran por especificación, esto en base a la VLAN que se utilice.
- Tener un registro verdadero acerca de la red que quede establecida; para de ahí poder partir en datos fiables tanto en programación de VLAN´s, equipos, periféricos, convertidores de medios.
- Que los departamentos a los que se les brinda apoyo por medio de la red tengan mejor accesibilidad al medio y un campo de trabajo más confiable, pudiendo así agilizar sus órdenes de trabajo.
- Hacer de la red LAN un sistema de comunicación más robusto y organizado con el tendido del nuevo cableado estructurado 6 A en la caseta de control.
- Ausencia de interferencias electromagnéticas por medio del cableado estructurado con cable categoría 6 A.
- Lograr una red idónea para que en su momento si se quieren homologar segmentos de red para trabajar a par con redes externas lo pueda hacer sin grandes cambios más que en algún protocolo dentro de la configuración al puerto indicado mediante programación.
- Crear una barrera de alto nivel de seguridad en los puertos asignados a las VLAN's del departamento de Control y Protección y Medición mediante equipos Firewall programables los cuales aparte de la protección que nos da la VLAN.
- Dividir la subred de protecciones en tres VLAN's en las cuales se separaran tres tipos de procesos; protección de relés ,medición y PMU

1.3 ALCANCES Y LIMITACIONES

1.3.1 ALCANCES

Se tiene conocimiento en la práctica que el implementar switch capa tres con una adecuada segmentación de VLAN'S en una red de datos, nos proporciona un aumento de ancho de banda y un buen nivel de seguridad ,pero el hecho de que se implemente una configuración de red estandarizada en cuanto a periféricos, y bien estructurada re-organizando las VLAN'S

1.3.2 LIMITACIONES

Las limitaciones que se tienen contempladas en este proyecto se simplifican a tres puntos

- Con respecto a la optimización:

- Los equipos y periféricos de la red proporcionan un servicio de calidad con velocidades estándar con pocas caídas ya que la calidad de los equipos y la buena programación lo permiten, sin embargo esto no influye en el uso y recepción que se tenga por parte del usuario final ,por lo tanto para sacar el máximo provecho , es necesario en usuarios finales , tanto equipos adecuados , como usuarios que sepan hacer uso de este medio de manera correcta y configuración adecuada.

-Con respecto a la organización:

- Todas las conexiones ,periféricos y programación se plasman en estos diagramas, equipos que esta ligados a la red que hacen uso de redes inalámbricas y equipos que se anexen posteriormente en algún punto que lo permita se tendrán que anexar a los diagramas de manera posterior si se desea contar con información completa.

-con respecto a la seguridad

- El nivel de seguridad es alto partiendo incluso desde la red superior a la que se enlaza la LAN en la que se está trabajando, la cual también está totalmente asilada y protegida contra acciones hostiles y dañinas por parte de usuario y equipos externos sin embargo una vez trabajando desde adentro de esas barreras incluyendo las de las redes internas de la LAN protegidas por Firewalls los usuarios y equipos, tendrán la posibilidad de actuar de manera incorrecta sin que la seguridad implementada pueda intervenir para evitar el daño ,de ahí la importancia de saber cómo y qué departamento hace uso de la red.

1.5 HIPÓTESIS

Implementando la segmentación de la red datos mediante la creación de VLAN complementada con los cambios físicos de cableado estructurado y protección vía firewall logramos un nivel de optimización de una red de calidad profesional, con reducción de broadcast , aumento de banda ancha , una mejor organización, y reducción de interferencia electromagnética en la sala de control.

2. MARCO TEÓRICO

2.1 TIPOS DE REDES DE DATOS

Se denomina red de datos a aquellas infraestructuras o redes de comunicación de datos que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

2.1.1 DE ACUERDO A SU DISTRIBUCION

Las redes de datos se diseñan y construyen en arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la conmutación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física.

Red de Área Local (LAN): Las redes de área local suelen ser una red limitada la conexión de equipos dentro de un único edificio, oficina o campus, la mayoría son de propiedad privada.

Red de Área Metropolitana (MAN): Las redes de área metropolitanas están diseñadas para la conexión de equipos a lo largo de una ciudad entera. Una red MAN puede ser una única red que interconecte varias redes de área local LAN's resultando en una red mayor. Por ello, una MAN puede ser propiedad exclusivamente de una misma compañía privada, o puede ser una red de servicio público que conecte redes públicas y privadas. [1]

Red de Área Extensa (WAN): Las Redes de área extensa son aquellas que proporcionen un medio de transmisión a lo largo de grandes extensiones geográficas (regional, nacional e incluso internacional). Una red WAN generalmente utiliza redes de servicio público y redes privadas y que pueden extenderse alrededor del globo.

Red de Área Local Inalámbrica (WLAN): Una red de área local inalámbrica, también conocida como WLAN (del inglés Wireless Local Area Network), es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas. Usan tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Estas redes van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

El objetivo de una red de datos consiste en facilitar la consecución de un incremento de la productividad vinculando todas las computadoras y redes de computadoras de manera que los usuarios pueden tener acceso a la información con independencia del tiempo, ubicación y tipo de equipo informático.

2.1.2 TOPOLOGÍA DE REDES

Los tipos de redes de datos como se describe en “Red de Datos” se pueden clasificar de acuerdo a su expansión territorial y alcance geográfico, sin embargo en cuanto a redes LAN principalmente las podemos catalogar por la forma de su estructura, de equipos, cables y demás componentes de una red.

El tipo de topología utilizada afecta al tipo y capacidades del hardware de la red, su administración y las posibilidades de una expansión futura.

Las tres topologías más ampliamente usadas son:

Lineal (Bus)

Estrella (Star)

Anillo (Ring)

Lineal

(Bus): Topología de ducto (bus)
Una topología de ducto o bus está caracterizada por una dorsal principal con dispositivos de red interconectados a lo largo de la dorsal. Las redes de ductos son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo en el ducto, y entonces ellas envían sus paquetes de información. Las redes de ducto basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión) típicamente emplean la arquitectura de red ETHERNET.

Las redes de bus comúnmente utilizan cable coaxial como medio de comunicación, las computadoras se contaban al ducto mediante un conector BNC en forma de T. En el extremo de la red se ponía un terminador (si se utilizaba un cable de 50 ohm, se ponía un terminador de 50 ohms también).

Las redes de ducto son fáciles de instalar y de extender. Son muy susceptibles a quebraduras de cable, conectores y cortos en el cable que son muy difíciles de encontrar. Un problema físico en la red, tal como un conector T, puede tumbar toda la red.

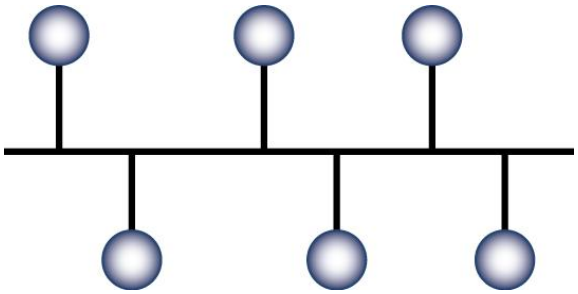

FIG. 2.1.2.1

Estrella: Topología de estrella (star)

En una topología de estrella, las computadoras en la red se conectan a un dispositivo central conocido como concentrador (hub en inglés) o a un conmutador de paquetes (swicth en inglés).
En un ambiente LAN cada computadora se conecta con su propio cable (típicamente par trenzado) a un puerto del hub o switch. Este tipo de red sigue siendo pasiva, utilizando un método basado en contención, las computadoras escuchan el cable y contienden por un tiempo de transmisión.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch (aunque se pueden conectar hubs o switchs en cadena para así incrementar el número de puertos). La desventaja de esta topología en la centralización de la comunicación, ya que si el hub falla, toda la red se cae.
Hay que aclarar que aunque la topología física de una red Ethernet basada en hub es estrella, la topología lógica sigue siendo basada en ducto.

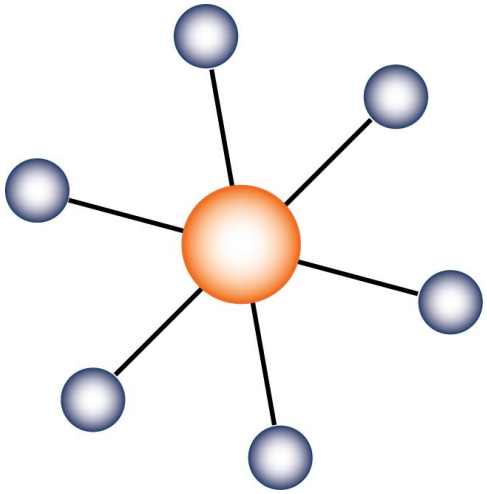

FIG. 2.1.2.2

Anillo: Topología de anillo (ring)

Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y posiciona de él. La computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje (a la computadora que envió los datos) que dé fueron recibidos correctamente.
La computadora que transmitió los datos, crea un nuevo token y los envía a la siguiente computadora, empezando el ritual de paso de token o estafeta (token passing) nuevamente.