ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERIA

ANÁLISIS Y DISEÑO DE UNA INFRAESTRUCTURA DE REDES BASADO EN VLAN´S PARA LA COMANDANCIA DEL EJÉRCITO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES DE INFORMACIÓN

MORALES GARRIDO MARCO

TAIPE TACO FABIAN

DIRECTOR: ING. RODRIGO CHANCUSIG.

Quito, Enero 2006

DECLARACIÓN

Nosotros, Vinicio Morales Garrido y Fabián Taipe Taco, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

MORALES GARRIDO MARCO VINICIO

TAIPE TACO FABIAN

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Morales Garrido Marco Vinicio y Taipe Taco Fabián bajo mi supervisión.

Ing. Rodrigo Chancusig

DIRECTOR DE PROYECTO

DEDICATORIA

A Dios, a mi amada esposa he hijos por la comprensión, paciencia y apoyo incondicional que me han demostrado en el trascurso de este tiempo, a mis padres, hermanos que contribuyeron con su apoyo, brindándome la oportunidad de cumplir una meta más en mi vida.

Marco Vinicio Morales

DEDICATORIA

A Dios, a mis padres, hermanos, que me apoyaron para llegar a cumplir una meta más en mi vida.

Fabián Taipe

AGRADECIMIENTOS

A la Escuela Politécnica Nacional, profesores de la carrera, quienes nos han compartido sus conocimientos técnicos y científicos para ser cada día mejores y útiles para la sociedad y el país.

A la Comandancia General de la Fuerza Terrestre por permitirnos realizar nuestro proyecto de titulación.

Al Sr. Capitán Hugo Álvarez encargado del Departamento de Comunicaciones por brindarnos todo su apoyo en la realización de este proyecto.

Al Ingeniero Rodrigo Chancusig por ser una de las personas más importantes en el desarrollo de este proyecto quien con sus conocimientos nos guió a la culminación de este trabajo.

LOS AUTORES

CONTENIDO

INDICES DE TABLAS

INDICES DE FIGURAS

RESUMEN

El presente proyecto tiene el propósito de optimizar los recursos computacionales con la que cuenta la institución mediante el análisis de la infraestructura, los requerimientos, y el planteamiento de un diseño que satisfaga las necesidades que actualmente requiere la CGFT mediante la utilización de la tecnología de las VLANs, y proponer recomendaciones de políticas de administración y seguridad de la red informática. También la utilización de un firewall en las Vlans que sean críticas. A continuación se describirán un resumen del contenido de cada capítulo que consta el proyecto.

En el capítulo 1, considera una introducción a las nuevas tendencias de las redes informáticas y su utilización. El uso de tecnologías VLANs, su clasificación de acuerdo a esquemas de configuración, la estandarización y arquitecturas que se utilizan en la implementación. Finalmente se realiza un cuadro comparativo de esta tecnología.

El capítulo 2, considera el análisis de la CGFT mediante la utilización de una metodología que establece su estructura orgánica funcional, la red informática actual, servicios y aplicaciones que presta, un inventario de usuarios, y una lista de los requerimientos demandados por la institución.

El capítulo 3, propone un diseño lógico y físico para los requerimientos establecidos por la CGFT, los equipos activos requeridos, las características técnicas de estos, recomendaciones de implementación, recomendaciones de políticas de seguridad y administración de la red informática propuesta.

El capítulo 4, establece un prototipo que refleja el diseño propuesto, la configuración de los equipos activos que se utilizan en la implementación del prototipo. Finalmente se establece las principales conclusiones y recomendaciones a las que se ha llegado para finalizar de manera satisfactoria el proyecto.

CAPÍTULO I

INTRODUCCION

La globalización, la Internet, la constante evolución de la tecnología y la necesidad que tiene el hombre de comunicarse y proteger la información que genera, le ha obligado a tomar acciones y decisiones enfocadas a compartir dicha información pero de una manera adecuada y segura, sobre ambientes confiables diseñados en base al uso de tecnologías de redes y de comunicaciones.

En la actualidad al interior de las empresas se genera gran cantidad de información, haciendo necesario el uso de múltiples servicios, como la mensajería electrónica, respaldos de datos, compartir recursos físicos y lógicos, la administración, la telefonía, entre los más usados. Para tener un comportamiento adecuado de dichos servicios se hace necesario un manejo eficiente, rápido, y seguro de dicha información por medio de infraestructuras tecnológicas de hardware, software y comunicaciones que tiene esta orientación.

Hoy en día, el intercambio de información a nivel de datos, voz y video es tan indispensable, que ha obligado a las empresas a contar con un sistema de cableado estructurado que brinden facilidades de mantenimiento, reubicación, administración y protección de la información. Sin embargo, tener un sistema de cableado estructurado que cumpla las normas y especificaciones, no garantiza el manejo eficiente, integridad y privacidad en la información, por lo que se necesita complementar su tratamiento con métodos de administración y protección basados en la segmentación de la red por medio de VLANs.

Toda empresa que posea una red, puede estar sujeto a un análisis, para determinar su estado actual, determinar los requerimientos en cuanto a usuarios y servicios, aspectos relacionados a la seguridad y la correcta administración por lo que los términos firewall[1], VPN´s[2], VLAN´s[3], serán usados de manera frecuente a lo largo de este trabajo.

Con ello, el Proyecto analizará la infraestructura actual de la Comandancia General de la Fuerza Terrestre (CGFT), enfocará los criterios y ventajas de implementar la tecnología de VLANs, mejorar los niveles de seguridad y la administración de la red con un diseño acorde e implementara un prototipo con la infraestructura básica que muestre el comportamiento mejorado de la red actual.

[1] **firewall**: “Es una combinación de técnicas, políticas de seguridad y tecnologías (hardware y software) encaminadas a proporcionar seguridad en la red, controlando el tráfico que circula entre dos o más redes”.

[2] **VPN.s:** “Proporciona el medio para usar una infraestructura de red pública como un canal apropiado para comunicaciones privadas de datos”.

[3] **VLAN´s:** “Son agrupaciones, definidas por software, de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus”.

1.2 FUNDAMENTO TEORICO

1.2.1 MODELO DE REFERENCIA OSI (OPEN SYSTEMS INTERCONECTION)

La Organización Internacional de Estándares (ISO), diseño el modelo de interconexión de sistemas abiertos (OSI), que es una guía para la elaboración de estándares de dispositivos de computadoras en redes. Con la finalidad que sean compatibles en un entorno multifabricante, con diferentes Sistemas Operativos y Protocolos. El modelo es de siete capas y cada una de las cuales cumple una función especifica y cada capa depende de la inmediata inferior. "[1]"

7 APLICACIÓN
6 PRESENTACION
5 SESION
4 TRANSPORTE
3 RED
2 ENLACE
1 FISICA

Figura 1.1: Modelo de referencia OSI

1.2.2 REDES LOCALES VIRTUALES (VLAN) "[2]"

Las VLANs son agrupaciones definidas por software y es un medio para dividir una red física (segmentación) en varias redes lógicas. Cada VLAN es un dominio de broadcast [4] (subred distinta) dentro del switch.

---

[4] **Broadcast:** "Sistema de entrega que proporciona la copia de un paquete dado a todos los anfritriones conectados para la difusión del paquete".

Las VLANs son principalmente usadas en control de broadcast, esto es, reduce el tráfico de broadcast en una red. La base de las VLANs esta en la utilización de switches[5] y ruteadores[6] que sirven para transmitir tráfico dentro de una VLAN y también para transmitir trafico entre diferentes VLANs.
Una forma de clasificación de las VLANs es de acuerdo a su configuración así se tiene: "[3]"

1.2.2.1 VLANs Estáticas

Las VLANs estáticas se estructuran con puertos de un switch que se asignan estáticamente a una VLAN. Estos puertos mantienen sus configuraciones de VLAN asignadas hasta que se cambien, necesitan de un administrador para realizar los cambios, es la más segura, de fácil configuración y monitoreo. Este tipo de configuración son propicias en redes en las que el movimiento de sus usuarios no es continuo por lo contrario es fijo.

[5] **Switch:** "Es un dispositivo diseñado para resolver problemas de rendimiento en la red. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC".

[6] **Routers:** "Es un dispositivo diseñado para segmentar la red, que limita el tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de brodcast. Opera en la capa 3 del modelo OSI".

Figura 1.2: Configuración de VLANs Estáticas [3]

1.2.2.2 VLANs Dinámicas

Las VLAN dinámicas son en las que los puertos del switch se pueden configurar dinámicamente y automáticamente con herramientas de software. Y la base de este tipo de configuraciones se lo realiza en: direcciones MAC, direccionamiento lógico o tipo de protocolo de los paquetes de datos.

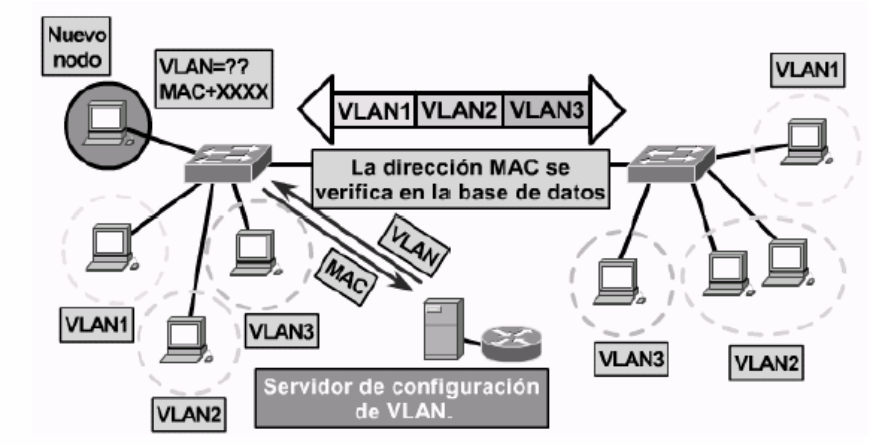


Figura 1.3: Configuración de VLANs Dinámica [3]

1.2.2.3 Beneficios de las VLANs "[4]"

Entre los principales beneficios se mencionan los siguientes: "[5]"

- Reduce en forma relativa los costos de administración relacionados con movimiento, adición o cambios de usuarios. Este beneficio es cuando las VLANs han sido implementadas en el nivel 3 con direcciones IP.
- Aumento de seguridad de la red de la organización, como también en los grupos de trabajo, siendo mayor cuando su configuración se lo realiza con puerto privado en un switch. También se puede implementar un firewall en cada VLAN fácilmente, esto es, un servidor encargado de la seguridad, que establece permisos de entrada a cada red virtual.
- Se puede establecer grupos de trabajo virtuales en una misma red LAN física, es decir, las estaciones de trabajo pueden estar físicamente contiguos pero están en diferentes VLANs.
- Control y conservación del ancho de banda, las VLANs puede restringir los broadcast a los dominios lógicos donde ha sido generados. Además, añadir usuarios a un dominio determinado o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- Con los procesos de reingeniería de empresas y de downsizing, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes.
- Se puede controlar el tráfico de broadcast de 2 maneras: limitando el número de puertos en el Switch o limitando el número de estaciones de trabajo que usan los puertos. Estas diferencias entre los 2 tipos de redes hace de las redes virtuales sean la solución más económica desde el punto de vista de desempeño y rapidez del flujo de información.
- Reutilización de inversión existente porque la implementación no requiere cambios en la estructura de la red o cableado, sino mas bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales.

- Se tiene una mayor administración y control de todos los recursos, aplicaciones y usuarios que se encuentran en la organización porque su administración es centralizada.

1.3 ESTÁNDARES

1.3.1 ESTANDARIZACIÓN DE REDES LAN

La IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) ha estandarizado la mayoría de las redes LANs mediante el Comité denominado 802. Este Comité ha desarrollado estándares a nivel de las capas 1 y 2 del modelo OSI, con la finalidad de que diferentes fabricantes puedan trabajar juntos e integrarse sin problemas.

Este Comité esta dividido en subcomités, cuyo nombre oficial es Grupos de Trabajo, que se identifican por un número decimal. Los grupos de trabajo 802 continuamente están planteando nuevas técnicas y protocolos para su estandarización, nuevos medios físicos. Al surgir una propuesta, el grupo correspondiente nombra un grupo de estudio que la analiza, y si el informe es favorable se crea un subgrupo que eventualmente propone un adendum al estándar para su aprobación. Los proyectos se identifican por letras añadidas al grupo de trabajo del que provienen. “[6]“

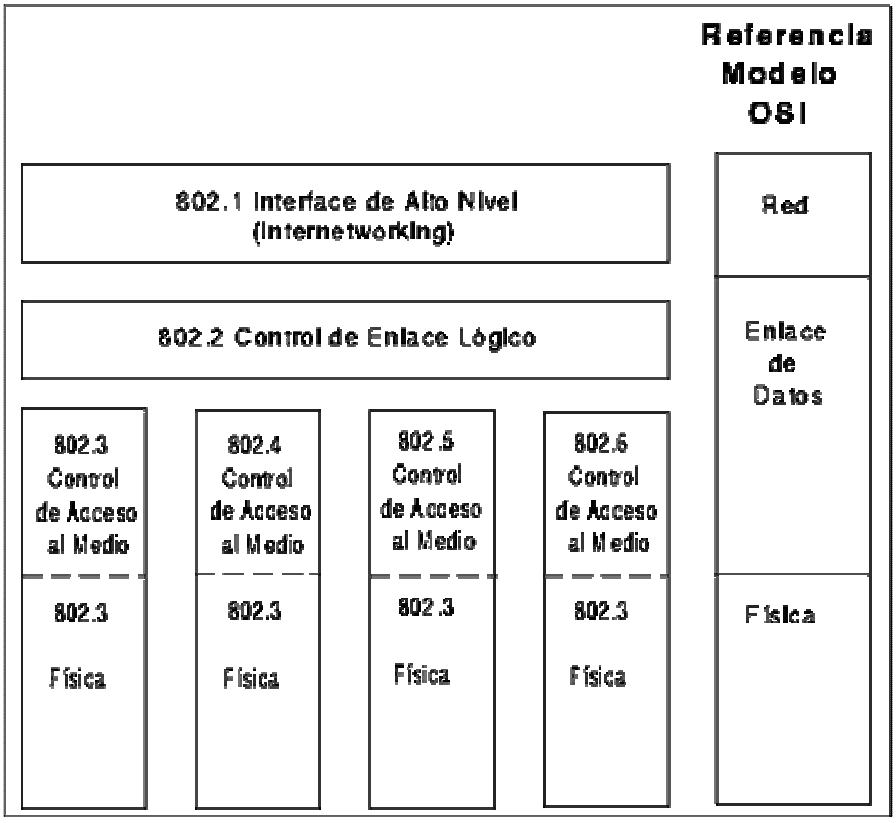


Figura 1.4: Estandarización de las redes Lan con referencia al Modelo OSI [6]

Grupos de trabajo.

802.1 Protocolos superiores de redes de área local

802.2 Control de enlace lógico

802.3 Ethernet

802.4 Token Bus (abandonado)

802.5 Token Ring

802.6 Red de área metropolitana (abandonado)

802.7 Grupo de Asesoría Técnica sobre banda ancha (abandonado)

802.8 Grupo de Asesoría Técnica sobre fibra óptica (abandonado)

802.9 RAL de servicios integrados (abandonado)

802.10 Seguridad interoperable en LAN(abandonado)

802.11 Red local inalámbrica, también conocido como Wi-Fi

802.12 Prioridad de demanda

802.14 Cable modems, es decir modems para televisión por cable. (Abandonado)

802.15 Red de área personal inalámbrica, (Bluetooth, entre otros)

802.16 Acceso inalámbrico de Banda Ancha, también llamada WiMAX, para acceso inalámbrico desde casa.

802.17 Anillos de paquetes con recuperación, se supone que esto es aplicable a cualquier tamaño de red, y está bastante orientado a anillos de fibra óptica.

802.18 Grupo de Asesoría Técnica sobre Normativas de Radio

802.19 Grupo de Asesoría Técnica sobre Coexistencia.

802.20 Acceso inalámbrico de Banda ancha móvil, que viene a ser como el 802.16 pero en movimiento.

802.21 Interoperabilidad independiente del medio

802.22 Red inalámbrica de área regional.

Proyectos:

- 802.1d: puentes transparentes
- 802.1g: puentes remotos
- 802.1p: Filtrado por clase de tráfico (Calidad de Servicio)

- 802.1q: Redes locales virtuales (VLANs)
- 802.3u: Fast Ethernet
- 802.3x. Ethernet Full dúplex y control de flujo
- 802.3z: Gigabit Ethernet
- 802.3ab: Gigabit Ethernet en cable UTP-5
- 802.3ae: 10 Gigabit Ethernet

1.3.1.1 Estandarización en VLANs

En un inicio cada fabricante desarrollaba su propia tecnología de VLAN de acuerdo a sus necesidades, lo que implicaba la incompatibilidad entre fabricantes, obligando a los usuarios a ser dependientes de un único proveedor, razón por la cual se vio la necesidad de la estandarización de esta tecnología.

Así, en el año de 1995 la empresa Cisco Systems propone el uso del IEEE 802.1, que fue originalmente establecido para direccionar las LAN dentro de las VLAN, tomando el formato de cabecera de la trama y evitando el transporte de la trama etiquetada. Aunque esta idea trabajaba técnicamente, la mayoría de los miembros del comité de la 802 se opuso, ya que el proceso de la trama era más difícil y más lento y por lo tanto más costoso.

En marzo de 1996 el subcomité de interacción de redes de la IEEE 802.1 completa la fase de investigación para el desarrollo de los estándares de las VLAN, concretando sus resoluciones en tres ideas básicas:

- La arquitectura de las VLANS.
- El formato estandarizado para el etiquetamiento de las tramas con el fin comunicar a los miembros de las VLANs a través de dispositivos de diferentes fabricantes, conocido como 802.1Q;
- Las futuras estandarizaciones de las VLANS.

1.3.1.2 IEEE 802.1Q [7]

Estándar recomendado por la IEEE para etiquetado de tramas VLANs. Permite transmitir en las tramas Ethernet la información de VLAN. Conceptualmente es simple: se agregan a la trama Ethernet 4 bytes. La figura muestra una trama Ethernet "normal" y una trama Ethernet 802.1q:

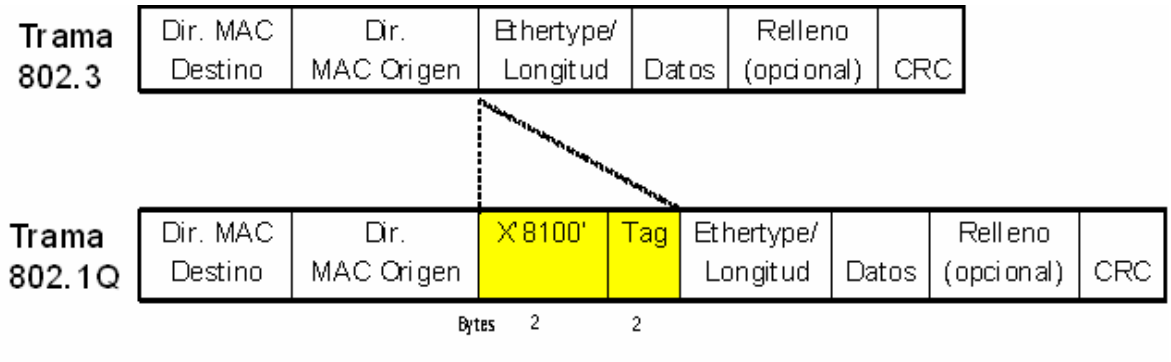


Figura 1.5: Etiquetado de trama según 802.1Q [7]

En la figura 1.5 se puede observar que se agregan 4 bytes: los primeros 2, que son fijos e identifican a la trama como una trama 802.1q. Los segundos 2 bytes, llamados "TAG" (marca o etiqueta) se interpretan como 3 conjuntos de bits, de longitud 3 bits, 1 bit y 12 bits respectivamente:

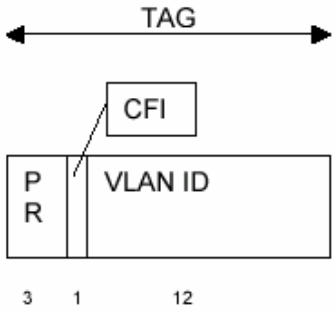


Figura 1.6: Partes de la etiqueta TAG [7]

El la figura 1.6 los primeros 3 bits del "TAG" indican la "prioridad" (8 niveles posibles), de acuerdo a la recomendación IEEE 802.1p [10]. El cuarto bit, llamado CFI (Canonical Format Indicator), indica formato de direcciones MAC.

Los últimos 12 bits indican la VLAN a la cual pertenece la trama. Estos 12 bits permiten tener, por lo tanto hasta 4096 VLANs. De esta manera, las tramas intercambiadas entre switches pueden contener información de VLAN.

1.3.1.3 Estándar IEEE 802.1p [8]

Es una extensión del Estándar 802.1d y se aplica para tratar con distintas prioridades al tráfico Ethernet (Calidad de Servicio (QoS)). Es utilizado en, aplicaciones de tiempo real, tales como: voz o video sobre Ethernet.

1.3.1.4 Estándar IEEE 802.1d [9]

La Recomendación IEEE 802.1d. Es un protocolo que permite crear una VLAN con equipos conectados a diferentes switches llamado “Spanning Tree”. La idea de este algoritmo es bloquear los enlaces que cierran los bucles, dejando a la red siempre con una topología del tipo “árbol”, y asegurar de esta manera que no existan bucles.

El algoritmo reevalúa periódicamente que enlaces hay que bloquear o rehabilitar para tener acceso a todos los equipos sin crear bucles. Por ello, utilizando adecuadamente el algoritmo “Spanning Tree” es posible armar explícitamente configuraciones en bucle que permitan tener enlaces de respaldo en caso de falla en los enlaces principales. Dado que el algoritmo permite valorar los enlaces con “pesos”, cuando existen bucles es posible configurar a prioridad que enlaces serán los principales y que enlaces quedarán bloqueados.

1.4 TECNOLOGÍAS EN LA IMPLEMENTACION DE VLANs

El desarrollo de las Redes Virtuales VLANs es nuevo, y el uso que se esta dando a nivel mundial en la reducción del dominio de colisión, aumento de la seguridad de la información entre grupos de trabajo dentro de las organizaciones, esta siendo ya explotados. Existen diferentes maneras de implementar redes VLANs a través de productos conmutados (Switches), cada una con diferentes capacidades y limitaciones.

Tipos de VLANs: "7"

- VLANs basadas en puertos
- VLANs de la capa MAC o control de acceso al medio
- VLANs de la capa de red
- VLANs de los IP o protocolos de Internet de múltiple mensaje (multicast).
- VLANs basadas en Reglas (POLICY BASED VLANS).

1.4.1 VLAN POR PUERTOS

En este tipo de Vlans cada puerto del conmutador (switch) puede asociarse a una VLAN. De esta manera, las máquinas conectadas a un puerto únicamente "ven" a las máquinas que están conectadas a Puertos de la misma VLAN. Tienen una tabla en la que asocian el número de puerto con el VLAN ID. Su principal desventaja es que no permite movilidad, ya que si un usuario se cambia, se debe reasignar el puerto para que éste siga en la misma VLAN.

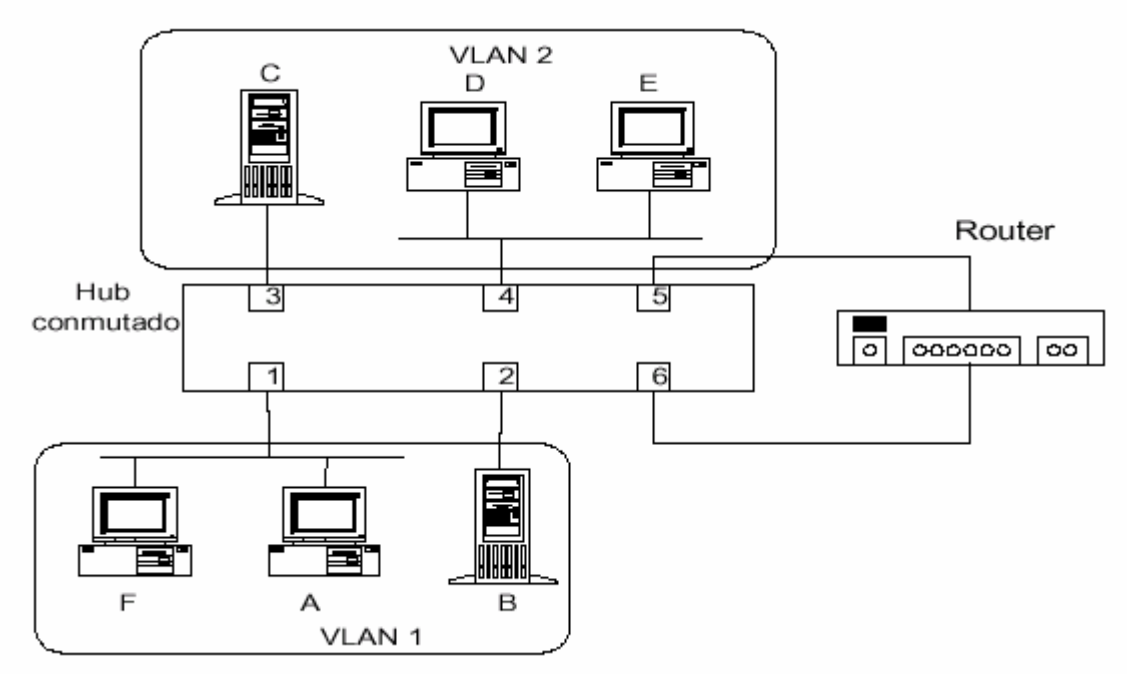


Figura 1.7: VLAN por puertos "7"

1.4.2 VLAN POR DIRECCIONES MAC

Aquí las direcciones MAC se asocian para formar VLANs. De esta forma, se pude restringir la red únicamente a ciertas direcciones MAC, independientemente al puerto del switch que este conectado, su principal ventaja es que permite movilidad para los usuarios.

1.4.3 VLAN POR PROTOCOLO

Se basa en información del campo Protocol Type del frame que resulta al inspeccionar datos de la capa 3, así por ejemplo tenemos IP, IPX, etc. Por lo tanto, el equipo mantiene una tabla en la que existe una relación entre el protocolo de nivel de red y el VLAN ID. Una de las ventajas para los administradores es que permite el particionado por tipo de protocolo cuando utilizan una estrategia de VLAN basada en servicios o aplicaciones.

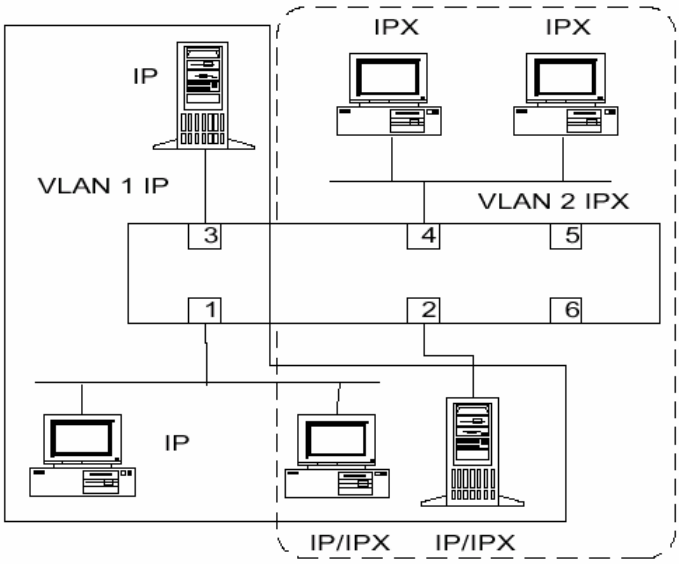


Figura 1.8: VLAN por protocolo "7"

1.4.4 VLAN POR DIRECCIONES IP

Estas VLAN se asocian a la dirección de red o de subred que tenga el equipo su configuración se realiza dinámicamente. Esto se presta para que las VLAN trasciendan a conexiones a nivel de WANs.

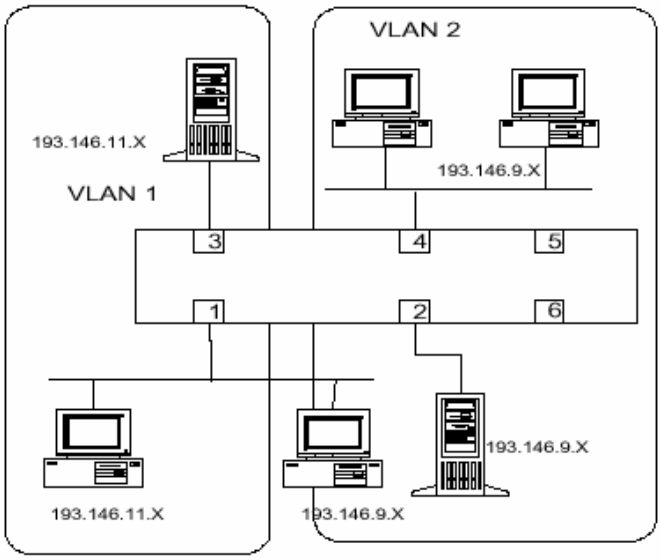


Figura 1.9: VLAN por direcciones IP "7"

1.4.5 VLANS BASADAS EN REGLAS (POLICY BASED VLANS).

Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

1.5 ARQUITECTURAS DE LAS VLANS

En la actualidad existen dos arquitecturas VLANs que son las mas conocidas y difundidas y que son: Implementaciones infraestructurales de VLANs y Implementaciones de VLAN basadas en el servicio.

1.5.1 IMPLEMENTACIONES INFRAESTRUCTURALES DE VLANS [5]

Se basa en la estrategia tradicional de las VLANs, el formar grupos de trabajo de acuerdo a como están distribuidas las organizaciones. Cada grupo, departamento o sección tiene unívocamente definida su VLAN y basado en la regla del 80/20, es decir, se asume que la mayoría de tráfico se da dentro de la VLAN.

Normalmente existirán sobrelapamientos al acceder fuentes comunes a todas las VLAN, lo cual se resolverá al ubicar estos recursos en servidores; Evitando que se empleen Routers para poder controlar el tráfico que accede a los recursos.

Entre las ventajas que se puede tener de este tipo de implementación son: Administración sencilla y centralizada, permite mantener fronteras

organizacionales discretas, bajo costo de desarrollo, buen grado de privacidad y permite alcanzar una alta eficiencia de la red.

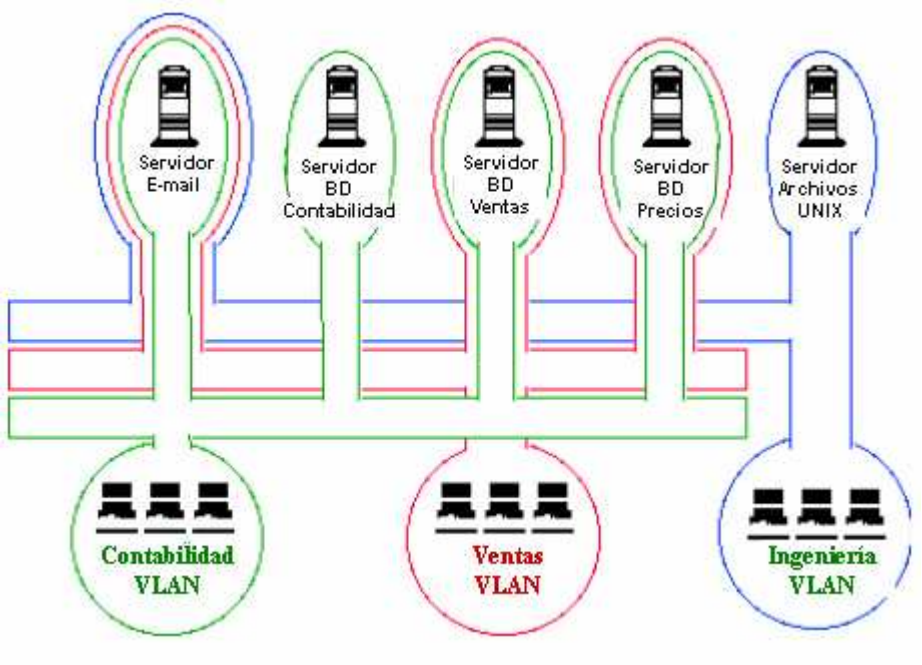


Figura 1.10: Implementación Infraestructural "5"

1.5.2 IMPLEMENTACIÓN BASADA EN EL SERVICIO

En la implementación basada en el servicio, no se tienen grupos o algo similar, cada VLAN presta un servicio, es responsable de administrar un recurso específico y ningún servidor podrá pertenecer a múltiples VLANs.

El acceso de los usuarios a los servicios de correo, bases de datos, aplicaciones, se hace a través de una VLAN independiente.

Esta implementación es de naturaleza dinámica comparada con la anterior arquitectura implicando serios inconvenientes para administrar la memoria a cada VLAN, porque esto conlleva a un alto grado de automatización en la configuración de las VLANs. También Las VLANs perderán la característica estática o semi-estática de dominios previamente definidos.

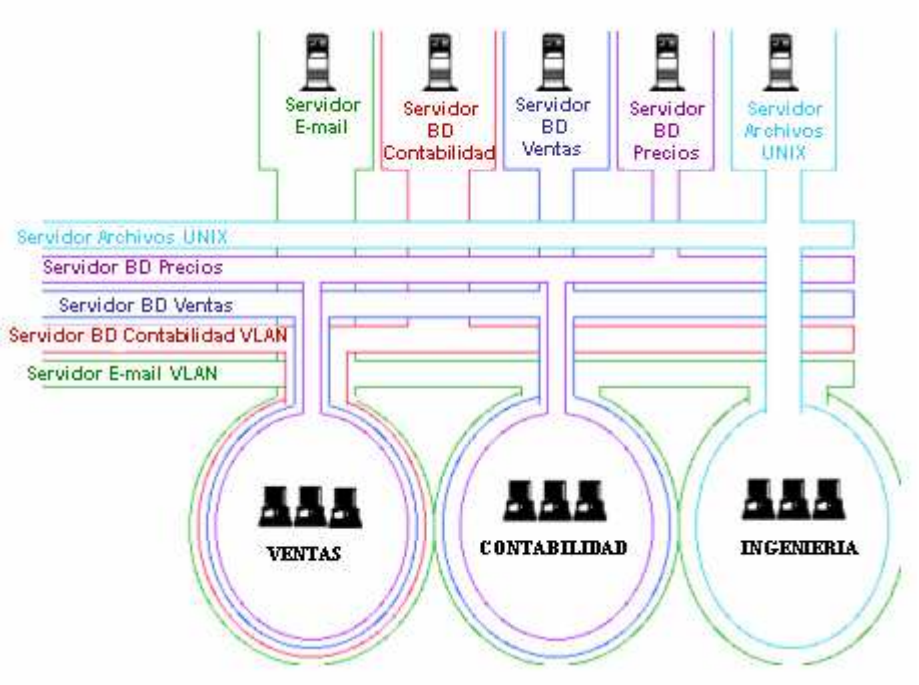


Figura 1.11: Implementación Basada en el Servicio "5"

También se puede implementar VLANs combinando estos dos modelos es decir VLANS infraestructurales con VLANs de servicios o viceversa según las necesidades de la organización.

1.6 CUADRO COMPARATIVO DE LAS CARACTERISTICAS IMPORTANTES DE LOS TIPOS DE VLANs "10"

TIPO DE VLAN / característica	PUERTOS	DIRECCIONES MAC	PROTOCOLO	DIRECCIONES IP	POLITICAS
Flexibilidad	no	moderada	Moderada	moderada	mucho
Seguridad	alta	mínima	Mínima	mínima	seleccionable
Movimiento de equipos	no	si	Si	si	automática
Número de VLANs	limitado	posible	Posible	posible	automática
Fácil asignación	si	no	Si	variable	si

Tabla 1.1: Características importantes los tipos de VLANs "10"

CAPÍTULO II

2.1 ANALISIS Y REQUERIMIENTOS DE LA ORGANIZACIÓN

En este capítulo utilizará una metodología que permitirá analizar la estructura tecnológica actual de la CGFT, proyectando con ello una mejor alternativa tecnológica a aplicarse. Para esto, se recopilará la información relacionada a la red informática actual, sus servicios, usuarios, equipos activos y pasivos. Al final se identificará los nuevos requerimientos solicitados por el administrador de la red y personal técnico involucrado.

2.1.1 METODOLOGÍA

La utilización de una metodología de análisis, es muy importante en toda investigación científica porque nos permite adquirir nuevos conocimientos y resolver los problemas planteados.

Por tal razón se utilizará una ***metodología sistemática*** ”11” la misma que está estructurada en etapas, cada una de las cuales sirven de base para la siguiente etapa, para cumplir los objetivos generales planteados.

Las etapas que se plantea para este proyecto son:

- Análisis de la institución y requerimientos de la misma
- Diseño de una solución de acuerdo a los requerimientos
- Implementación de un prototipo

2.1.1.1 Análisis de la institución y requerimientos de la misma

Esta etapa comprende un estudio de la Institución, su estructura organizacional, un inventario de los usuarios que la conforman, como también un inventario de los recursos tecnológicos que dispone actualmente la institución.

Toda esta información se obtendrá a base de entrevistas y formularios, los mismos que estarán enfocados a establecer los principales requerimientos que la institución requiere.

2.1.1.2 Diseño de una solución de acuerdo a los requerimientos

Esta etapa comprende en establecer un diseño lógico y físico que cumpla los requerimientos demandados por la institución.

También en esta etapa se propone recomendaciones de implementación y políticas de administración para la red informática.

2.1.1.3 Implementación de un prototipo

En esta última etapa se implementa una parte del diseño propuesto, con la finalidad de realizar las pruebas respectivas. Llegando a obtener las principales conclusiones y recomendaciones de este proyecto

2.2 ANÁLISIS Y DIAGNOSTICO DE LA INFRAESTRUCTURA ACTUAL

Este estudio se ha hecho a base de entrevistas e información proporcionada por personal que conforma el departamento Comunicaciones, el cual esta a cargo de la administración de esta infraestructura y de proyectos a implementarse en un

futuro cercano en la red informática de la CGFT **ANEXO A** (ENTREVISTAS) **ANEXO B** (FORMATO DE ENTREVISTAS).

2.2.1 ENTORNO DE LA CGFT "[12]"

El edificio del CGFT, esta conformado de doce pisos incluyendo el subsuelo. En cada piso se han creado divisiones administrativas llamadas Direcciones, las mismas que se subdividen en Departamentos y cada uno de los cuales cumplen una función específica, permitiendo de esta manera delegar funciones a cada Dirección.

Este modelo de organización se lo ha realizado de esta forma porque permite controlar el ingreso de personas que visitan la Institución, así como al mismo personal que labora en ella debido a que la CFGT es una Institución que da seguridad nacional al país. La información que se maneja dentro de la Institución es muy confidencial y necesita mecanismos que permitan un control de las personas que ingresan a ella.

2.2.1.1 Direcciones Administrativas de la CGFT

Las Direcciones Administrativas con las que actualmente cuenta la CGFT son:

- Dirección de Operaciones de la Fuerza Terrestre (DOFT)
- Dirección de Logística de la Fuerza Terrestre (DLFT)
- Dirección de Comunicaciones de la Fuerza Terrestre (DICONSI)
- Dirección de Educación de la Fuerza Terrestre (DEFT)
- Dirección de Finanzas de la Fuerza Terrestre (DFFT)
- Dirección de Doctrina de la Fuerza Terrestre (DDFT)
- Dirección Bienestar de Personal de la Fuerza Terrestre (DBPFT)
- Dirección de Sanidad de la Fuerza Terrestre (DSFT)
- Compañía cuartel general de la Fuerza Terrestre (CCGFT)

Las Direcciones que están subdivididas en Departamentos todas ellas tienen una estructura similar de manera que es suficiente enfocarlas de manera general y no detallar con exactitud, debido a la seguridad, confidencialidad y restricciones que maneja la CGFT.

El organigrama que se puede observar en forma general de como esta estructurado y administrada la CGFT es:

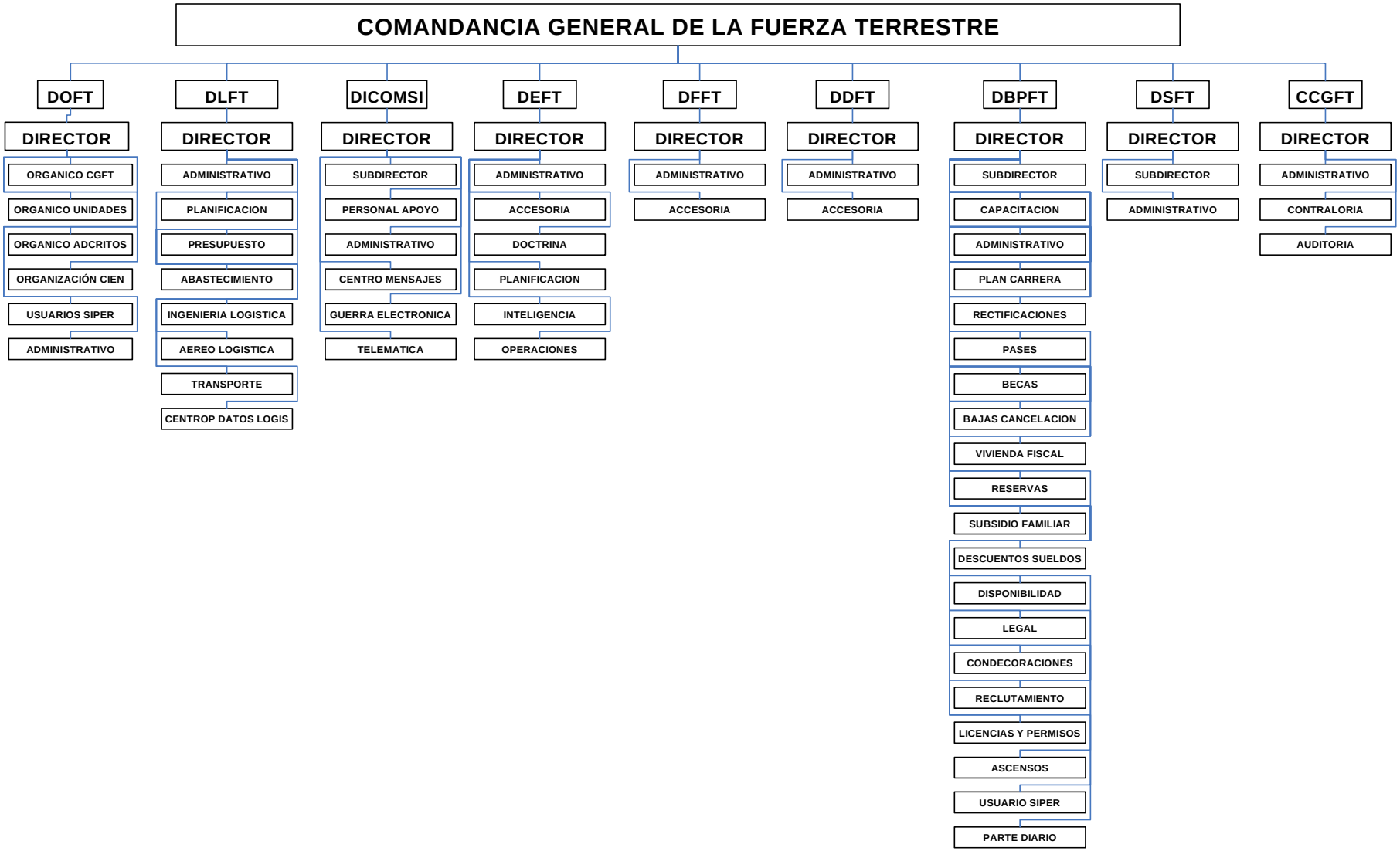


Figura 2.1: Organigrama Administrativo de la CGFT "12"

2.2.1.2 Red actual de la CGFT "12"

La red de la CGFT esta constituida por dos redes, la Intranet y la Internet las mismas que trabajan de forma independiente es decir poseen su propio cableado estructurado para prestar sus servicios y aplicaciones. En estas dos redes se encuentran distribuidos todos los usuarios que conforman la CGFT como lo son: personal de administración, personal técnico, usuarios de aplicaciones.

A su vez, el personal está subdividido en grupos que tienen diferentes objetivos y funciones, los que necesitan para el desarrollo de su trabajo diversos tipos de infraestructuras de red y comunicaciones.

2.2.2 RED INTERNET

La Red Internet está construida como una red independiente con: servidores de autenticación, autorización, acounting, E1 digital, RAS digital, firewall, encriptores (seguridad), software y un enlace al telépuerto de IMPSAT, este ISP provee un ancho de banda de 512 kb.

Los usuarios que tienen acceso al servicio de Internet son:

- 200 entre Directores, Subdirectores, Administrativos y usuario en general de la LAN de la CGFT.
- 541 usuarios entre Comandantes De Divisiones, Brigadas, a nivel nacional, correspondiente a unidades y repartos militares, para cuyos enlaces utilizan líneas del Sistema MODE (El Sistema MODE digital es el Sistema de comunicaciones de las Fuerzas Armadas). Este Sistema MODE es una red externa de enlaces equivalente a la red externa de Andinatel, pero es de administración y uso exclusivo de las Fuerzas Armadas.
- 50 utilizando las líneas de Andinatel, para acceso vía dial up de personal civil y militar desde sus domicilios.

2.2.3 RED INTRANET

Esta formada por un cableado estructurado categoría 6 en cada uno de los pisos y se interconectan a través de un backbone de fibra óptica conectados a su vez a cada uno de los cuartos de comunicación.

Esta red tiene la finalidad de prestar a los usuarios los servicios y aplicaciones que la CGFT posee. Se tiene 80 usuarios distribuidos en toda la CGFT.
El siguiente grafico indica la distribución actual de la red Internet y la red Intranet de la CGFT.

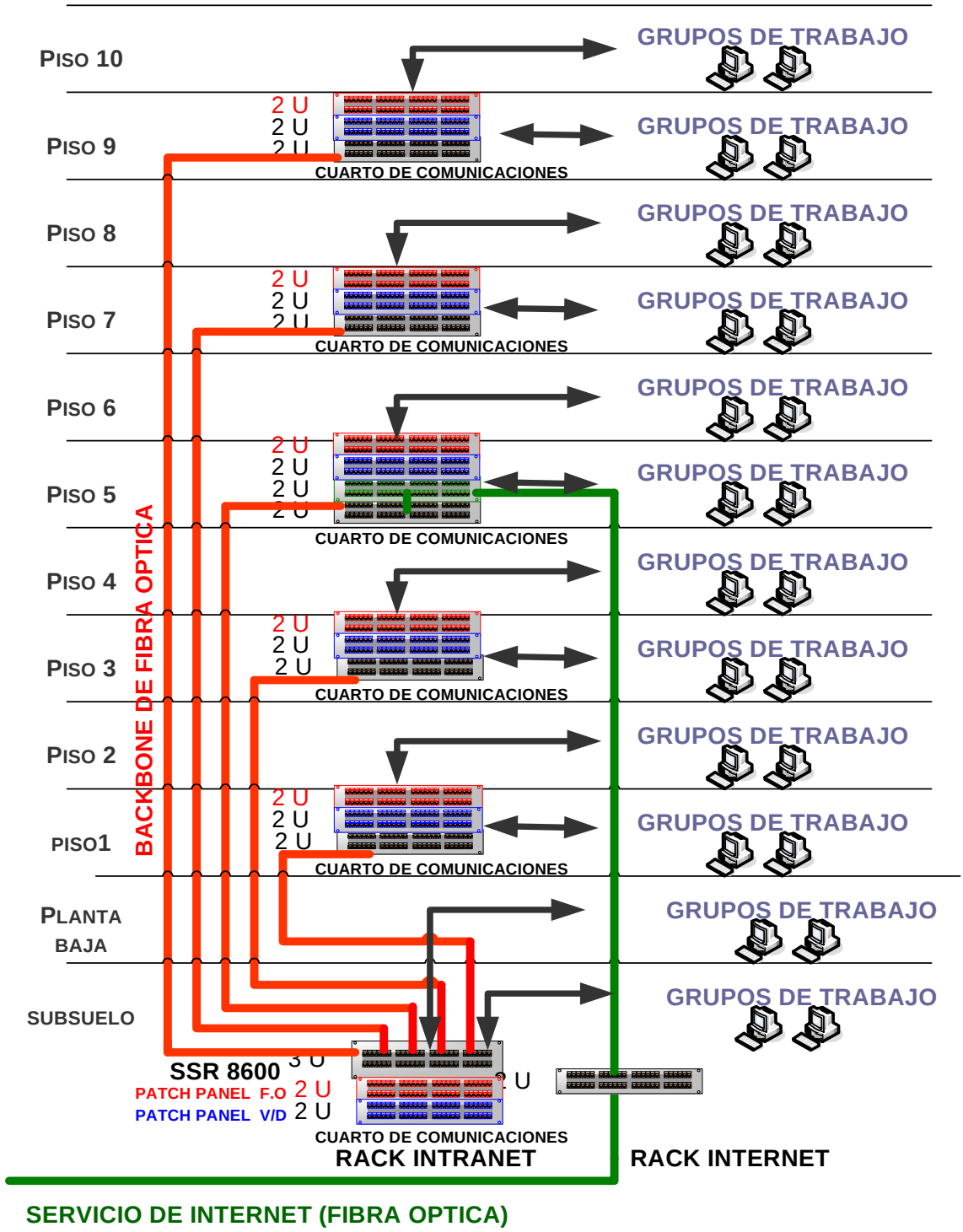


Figura 2.2: Distribución de las Redes Intranet e Internet

El listado general de todos los usuarios de la red Internet e Intranet que conforman la CGFT sus ubicaciones por piso, direcciones IP y que puertos utilizan se la puede observar en el **ANEXO C** (INVENTARIO USUARIOS CGFT)

2.2.4 OBSERVACIONES DE LA RED INTRANET E INTERNET

Hasta el momento podemos observar que la red informática de la CGFT no presta todos sus servicios y aplicaciones a todos los usuarios que conforman la institución debido a que las dos redes se encuentran trabajando de forma independiente y paralela por lo cual los recursos de red están siendo desperdiciados, además su administración es mas compleja debido al tipo de distribución operativa que este momento dispone.
La topología de red que actualmente dispone la CGFT tanto para la red intranet como para la red Internet es de tipo estrella,

2.3 ANÁLISIS DEL ENTORNO DE LA ORGANIZACIÓN

En este punto se analizará la distribución de los cuartos de telecomunicaciones, servidores que posee la institución, distribución de los switches en los diferentes pisos y un resumen de los servicios y aplicaciones de los mismos.

2.3.1 CUARTO DE TELECOMUNICACIONES

Estos cuartos de telecomunicaciones contienen los rack, patch panel, switches de piso tanto para la red de Internet como para la Intranet. Estos patch panels soportan voz, datos y video. Se encuentran en los siguientes pisos: subsuelo, pisos 1, 3, 5, 7 y 9.

2.3.2 SERVIDORES

2.3.2.2 Servidores de Internet

SERVIDOR	HARDWARE	DESCRIPCION
DNS	• CPU SUM MICROSYSTEM ULTRAS • MONITOR DE 15” • RISC DE 64 BITS	Es un servidor que se encarga de traducir nombres de sistema (como por ejemplo www.yahoo.com) en sus correspondientes direcciones IP. Para poder navegar por Internet.
Cache, Ftp	• SERV. DELL PEDGE2500 • DISCOS DE 18 GB • DISCOS DE 38 GB • MEMORIAS 1 GB • MONITOR DE 15”	El Server de cache es el encargado de atender las peticiones HTTP de los usuarios locales, sin la necesidad de transferir estas al enlace del ISP, optimizando de esta forma el uso del ancho de banda WAN y mejorando notablemente los tiempos de respuesta, almacena los sitios Web más solicitados por los usuarios.

Web, Mail	• SERV. DELL PEDGE2500 • 2 DISCOS DE 18 GB • 2 DISCOS DE 38 GB • MEMORIAS 1 GB • MONITOR DE 15”	El servidor Web es un programa que escucha las peticiones HTTP que le llegan y las satisface. Dependiendo del tipo de la petición, el servidor Web buscará una página Web o bien ejecutará un programa en el servidor. Este servidor Web es fundamental en el desarrollo de las aplicaciones del lado del servidor, server side applications, que se realice, ya que se ejecutarán en él. El servidor Mail es el encargado de contener todas las direcciones de los usuarios para que puedan enviar y recibir mensajes al exterior de la institución.
Respaldo Internet y Mail	• SERVIDOR SUN MODELO SPARC Station 5 • MEMORIA RAM 256 • 2 DISCO DUROS 36 GB • MONITOR DE 15” • RISC DE 32 BITS	Servidor que contiene los respaldos como: Bases de Datos de usuarios de Internet, correo.
Correo Militar	• COMPAQ DESKTOP • MONITOR DE 15”	Este servidor constituye un correo netamente interno, es el encargado de contener buzones de los usuarios militares, quienes envían y reciben mensajes netamente de carácter militar y confidencial.

WebSense	• PC CLON PIII , 1 GHZ DE VELOCIDAD, 160GB EN DISCO DURO, 512 MB EN RAM • MONITOR DE 15”	WebSense es el encargado de la administración y control de accesos a Internet, supervisa e informa acerca del uso de Internet por parte de los empleados.
Antivirus	• PC CLON PIII , 1 GHZ DE VELOCIDAD, 60GB EN DISCO DURO, 256 MB EN RAM • MONITOR DE 15”	Se encarga de disponer de software actualizado (antivirus) para todos los usuarios de la red con la finalidad de protegerse de ataques internos e externos (virus, gusanos, spoofing).
Event Viewer	• PC CLON PIII , 1 GHZ DE VELOCIDAD, 80GB EN DISCO DURO, 512 MB EN RAM • MONITOR DE 15”	Se encarga de recopilar y centralizar la información, que las aplicaciones recogen de los eventos de hardware o software, en unos archivos llamados log de eventos del sistema.

Tabla 2.1: servidores de la Internet

2.3.2.3 Servidores de la Intranet

SERVIDOR	HARDWARE	DESCRIPCION
SERVIDOR PRIMARIO DE APLICACIONES PROPIETARIAS DE LA CGFT	SUN 3500 • UNIDAD DE TAPE BACKUP EXTERNA • 3 DISCO 36 GB • 2 DISCO 18 GB • PROCESADOR 900 MHZ • RAM: 512 MB	Server de aplicaciones propietarias y base de datos, de la SIFT La CGFT dispone de una aplicación propietaria SIFT (Sistema Integrado de la Fuerza Terrestre) en la que se encuentran operativos los módulos de personal, recursos humanos, educación, adquisiciones, logística, los módulos para el resto de Direcciones se encuentran en proceso de desarrollo por parte de la ESPE.
SERVIDOR SECUNDARIO DE APLICACIONES PROPIETARIAS DE LA CGFT	SUN 450 • PROCESADORES PII RISC ULTRA SPARC DE 64 BIT • RAM: 512 MB • DISCOS ULTRA SCSI DE 36 GB, HOT PLUG • UNIDAD DE RESPALDO SUN 12-24 GB 4mm DDS-3 • SCSI TAPE UNIPACK EXTERNO	Este servidor Constituye el respaldo del servidor de aplicaciones propietarias de la CGFT

Tabla 2.2: Servidores de la Intranet

2.3.3 DISTRIBUCIÓN DE LOS EQUIPOS ACTIVOS

2.3.3.1 Distribución de equipos activos en la Internet

La distribución de los equipos activos que dispone actualmente la red Internet es la siguiente:

PISO	DESCRIPCION	# DE EQUIPOS	PUERTOS OCUPADOS
SUBSUELO	Switch Cisco 2950 24 puertos	1	16
1	Enterasys VH2402S 24 puertos	1	12
3	Switch Cisco 2950 24 puertos	1	15
5	Switch Cisco 2950 24 puertos	1	11
7	Switch Cisco 2950 24 puertos	1	15
9	Enterasys VH2402S 24 puertos	1	11

Tabla 2.3: Distribución de equipos activos de la Internet en la CGFT

2.3.3.2 Distribución de los equipos activos en la Intranet

La distribución de equipos activos en los cuartos de comunicaciones en todo el edificio de la CGFT es la siguiente:

PISO	DESCRIPCION	# DE EQUIPOS	PUERTOS OCUPADOS
SUBSUELO	Smart Switch Router 8600, 6 modulos de F.O.	1	6
SUBSUELO	Switch 3COM SuperStack 3878 48 puertos	1	22
1	Enterasys VH2402S 24 puertos	2	44
1	Enterasys VH2402S 24 puertos	1	19
3	Enterasys VH2402S 24 puertos	2	28
5	Enterasys VH2402S 24 puertos	2	31
7	Enterasys VH2402S 24 puertos	2	36
9	Enterasys VH2402S 24 puertos	2	24

Tabla 2.4: Distribución de equipos activos de la Intranet en la CGFT

2.3.4 APLICACIONES Y SERVICIOS DE LA CGFT

La CGFT dispone de una aplicación propietaria que es usada a nivel nacional, denominada SIFT (Sistema Integrado de la Fuerza Terrestre), este sistema esta construido en módulos de aplicaciones de acuerdo a necesidades y funciones de cada departamento de la CGFT, ejemplo, El Departamento de personal tiene aplicaciones para el control de: personal militar, licenciamientos, retiros, pases, este modulo es denominado SIPER (Sistema Integrado del Personal), el Departamento de logística controla inventarios de equipamiento militar a nivel nacional, este modulo es denominado SILOG (Sistema Integrado de Logística).

2.4 ANÁLISIS DE REQUERIMIENTOS EN RENDIMIENTO, SEGURIDAD Y CONECTIVIDAD

2.4.1 REQUERIMIENTOS DE RENDIMIENTO

- El esquema que actualmente tiene la CGFT es poco flexible debido a su utilización de dos redes independientes que son de Internet y Intranet.
- Con este tipo de esquema a existido un crecimiento desordenado en la red de datos de la CGFT desperdiciando puertos y recursos.
- El acceso a los servicios de la Internet se encuentran restringidos tecnológicamente a todos los usuarios que lo soliciten debido al esquema que esta implementado.

2.4.2 REQUERIMIENTOS DE SEGURIDAD

- Como consecuencia de este esquema se tiene una administración poco eficiente implicando los riesgos en la seguridad en la red informática de la CGFT.
- De los análisis anteriores se puede concluir que no se dispone de un diseño y topología de red definida que permita un crecimiento ordenado y permita la administración de la misma.
- Todos los recursos y facilidades que ofrece el Smart Switch Router 8600 no están explotados en su totalidad como es el caso que existe una poca utilización en la creación de VLANs. Debiendo ser necesario una mayor utilización debido a que este equipo activo solo se utiliza actualmente para una parte de la red informática.

2.4.3 REQUERIMIENTOS DE CONECTIVIDAD

- Los servidores que tienen sus aplicaciones necesitan conectarse a algunos grupos de de trabajo que se encuentran distribuidos en la CGFT y mantener un aislamiento entre grupos de trabajo.
- Al estar la CGFT distribuido en Direcciones se establecen grupos de trabajo en qué el mayor tráfico de información es en el mismo grupo y solamente un mínimo tráfico de información es entre grupos de trabajo.

2.4.5 ANÁLISIS DE EL TRÁFICO DE LA RED

Con la finalidad de realizar el análisis en la red informática se debe hacer uso de las herramientas de analizadores de red que sirven para mostrar el estado de la red en: trafico de red, direcciones IP, protocolos, ancho de banda de la red con esta información se puede establecer en que condiciones se encuentra la red.

Existen en el mercado gran cantidad de software para el análisis de una red informática. Existe software que se compran a un proveedor o software gratuito que se encuentra en las páginas Web.

Para optimizar recursos económicos a la institución se puede hacer uso de software gratuito. Para el análisis en la CGFT no fue permitido el uso de estos recursos por restricciones que se tiene para mantener confidencialidad en el manejo de la información por ser una institución de seguridad nacional.

En la siguiente tabla se mencionan algunos analizadores de red que se pueden utilizar:

HERRAMIENTA ADMINISTRATIVA	PLATAFORMAS	DESCRIPCION
MRTG (Multi Router Traffic Grapher)	WINDOWS LINUX	Es una herramienta para monitorizar el tráfico en las interfaces de red y representar gráficamente en páginas html con gráficos GIF los datos que obtiene de agentes SNMP o scripts
SNIFFER PRO 3.5	WINDO0WS	El sniffer Pro nos permite visualizar las siguientes tareas: • Aplicaciones • Sesiones • Conexiones • Estaciones • DLC's • Globales

Tabla 2.5: Software de administración de red

2.5 CONCLUSIONES

- Luego de realizar el análisis correspondiente a la CGFT se hace necesario la unificación de las dos redes.
- Se necesita optimizar los recursos que actualmente dispone la CGFT.
- Se debe establecer recomendaciones de políticas de administración y seguridad en la red informática de la CGFT.
- La información que se trasmite a través del cableado estructurado entre las diferentes Direcciones que conforman la CGFT debe ser trasmitida con la

confidencialidad necesaria, debido a que algunos grupos de trabajo no deben acceder a información de otros grupos de trabajo, por ejemplo: El grupo de trabajo de Finanzas debe estar aislado de los demás grupos de trabajo.

- Tener una red informática flexible, escalable y de fácil administración para el personal que esta a cargo de la administración.

CAPÍTULO III

3.1 DISEÑO Y PROPUESTA DE LA RED VLANS PARA LA ORGANIZACIÓN

3.1.1 INTRODUCCIÓN

Con el análisis, diagnostico de la infraestructura de la institución y requerimientos que ésta solicita, se ha llegado a establecer sus principales necesidades, así como también se ha obtenido un inventario del hardware que posee la institución hasta el momento.

En este capítulo se establecerá los principales beneficios que se puede obtener con una correcta utilización de los equipos activos que cuenta la CGFT tomando en cuenta la optimización de la infraestructura de cableado estructurado que posee y sobretodo proponer un esquema optimo de funcionamiento basado en VLANs para la red Intranet exclusivamente.

Por medio de la recopilación de información se ha llegado a la conclusión que la CGFT dispone de equipos activos de red de buena calidad y que su tecnología que posee puede cubrir los requerimientos solicitados, porque estos recursos aún no están explotados a su máximo rendimiento. Amerita una propuesta de diseño basado en VLANs que mejorará la operatividad de la red de la CGFT y de cumplir los requerimientos que solicita la institución tomando en cuenta la tecnología que poseen hasta el momento, costos de implementación y si es necesario se propondrá la compra de equipos si fuera necesario para mejorar y cumplir los requerimientos establecidos por la CFGT.

Finalmente se propondrá o recomendara de políticas de administración en seguridad que debería manejar la CGFT en relación a la información que maneja.

3.2 DISEÑO DE LAS VLANS EN LA ORGANIZACIÓN

Para establecer un diseño de VLANs, se partirá de un diseño lógico que cumpla los requerimientos establecidos para luego proponer un diseño físico que se adapte al diseño lógico.

3.2.1 DISEÑO LÓGICO DE LA RED

El diseño lógico que se propondrá a continuación será un esquema que permita una configuración flexible, con una administración sencilla y con niveles de seguridad aceptables y acorde a las ventajas que presentan los equipos activos de la CGFT.

Este diseño se basa en una Implementación infraestructural de VLANs debido a que esta arquitectura se adapta a los requerimientos antes establecidos.

Se dividirá la red en varias VLANs de acuerdo a las Direcciones y Departamentos que existen en la CGFT manteniendo la independencia necesaria entre VLANs, para el manejo de la información de las mismas.

Se hace necesario seis VLANs generales que prestarán todos los servicios que disponga la CGFT.

Estas VLANS son: Internet, Invitados, Switches, RAS, Servidores y Administración

Con el diseño propuesto se permitirá o negará el acceso a los usuarios que conforman la CGFT a los diferentes servicios, controlando, ruteando y permitiendo la comunicación entre las diferentes VLANs creadas, buscando con ello obtener estadísticas de tráfico para un adecuado control del funcionamiento de la red informática. Estas facilidades nos proporcionará el Smart Switch 8600.

El diseño lógico propuesto es el siguiente:

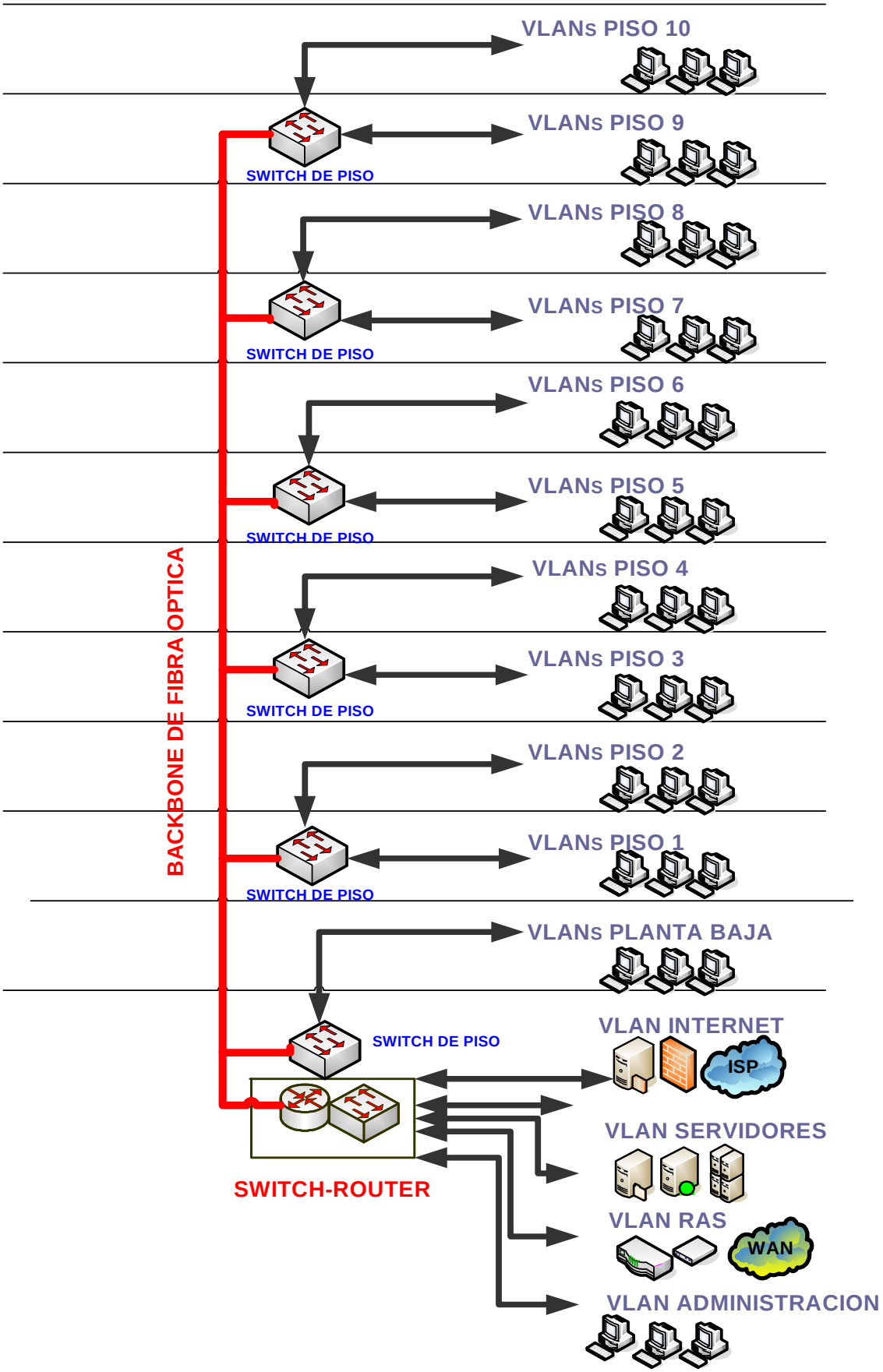


Figura 3.1: Diagrama lógico de la red VLANS propuesta

3.2.2 DISEÑO FÍSICO DE LA RED

En este punto se indica las Vlans propuestas y que se crearán en cada piso, incluyendo las seis VLANs generales que prestaran su servicio a todos los usuarios de la CGFT. El esquema propuesto de direcciones de la arquitectura interna que se usara es direcciones tipo C, 192.168.Número de VLAN.254 para identificar cada VLAN, como puerta de enlace de cada VLAN se asignara la siguiente dirección 192.168.Número de VLAN.253.

DISPOSITIVO	PISO	NOMBRE DE VLAN	ID VLAN	DIRECCION IP VLAN	GATE WAY
	10	CENTROMEN	101	192.168.101.254	192.168.200.254
		DOCTRINA	102	192.168.102.254	192.168.200.254
ENTERASYS	9	PLANIFICACION	103	192.168.103.254	192.168.200.254
VH2402S		ORGANIZACION	105	192.168.105.254	192.168.200.254
		ESPE	106	192.168.106.254	192.168.200.254
	8	COMUNICACIONES	107	192.168.107.254	192.168.200.254
		INSPECTORIA	108	192.168.108.254	192.168.200.254
ENTERASYS	7	INTELIGENCIA	109	192.168.109.254	192.168.200.254
VH2402S					
	6	COMUNICACIONSOCIAL	110	192.168.110.254	192.168.200.254
		EDUCACION	111	192.168.111.254	192.168.200.254
ENTERASYS	5	OPERACIONES	112	192.168.112.254	192.168.200.254
VH2402S		COMANDOCONTROL	113	192.168.113.254	192.168.200.254
	4	CIEMGENERAL	114	192.168.114.254	192.168.200.254
		JEFATURA	115	192.168.115.254	192.168.200.254
ENTERASYS	3	LOGISTICA	116	192.168.116.254	192.168.200.254
VH2402S					
	2	LOGISTICA2	118	192.168.118.254	192.168.200.254
	2	CUARTELGENERAL	119	192.168.119.254	192.168.200.254
		SANIDAD	120	192.168.120.254	192.168.200.254
ENTERASYS	1	RECURSOSHUMANOS	122	192.168.122.254	192.168.200.254
VH2402S					
	PB	BIENESTARPERSONAL	123	192.168.123.254	192.168.200.254
ENTERASYS	SUBS	SERVIDORES	125	192.168.125.254	192.168.200.254
VH2402S		ADMINISTRACION	126	192.168.126.254	192.168.200.254
		INVITADOS	127	192.168.127.254	192.168.200.254
		INTERNET	128	192.168..128.254	192.168.200.254
SMART SWICH		RAS	129	192.168.129.254	192.168.200.254
8600		TEMPORAL	130	192.168.130.254	192.168.200.254
		SWITCH	200	192.168.200.1	192.168.200.254

Tabla3.1: Propuesta de creación de VLANs para la CGFT

El siguiente diagrama muestra las VLANs propuestas y su distribución en los respectivos pisos:

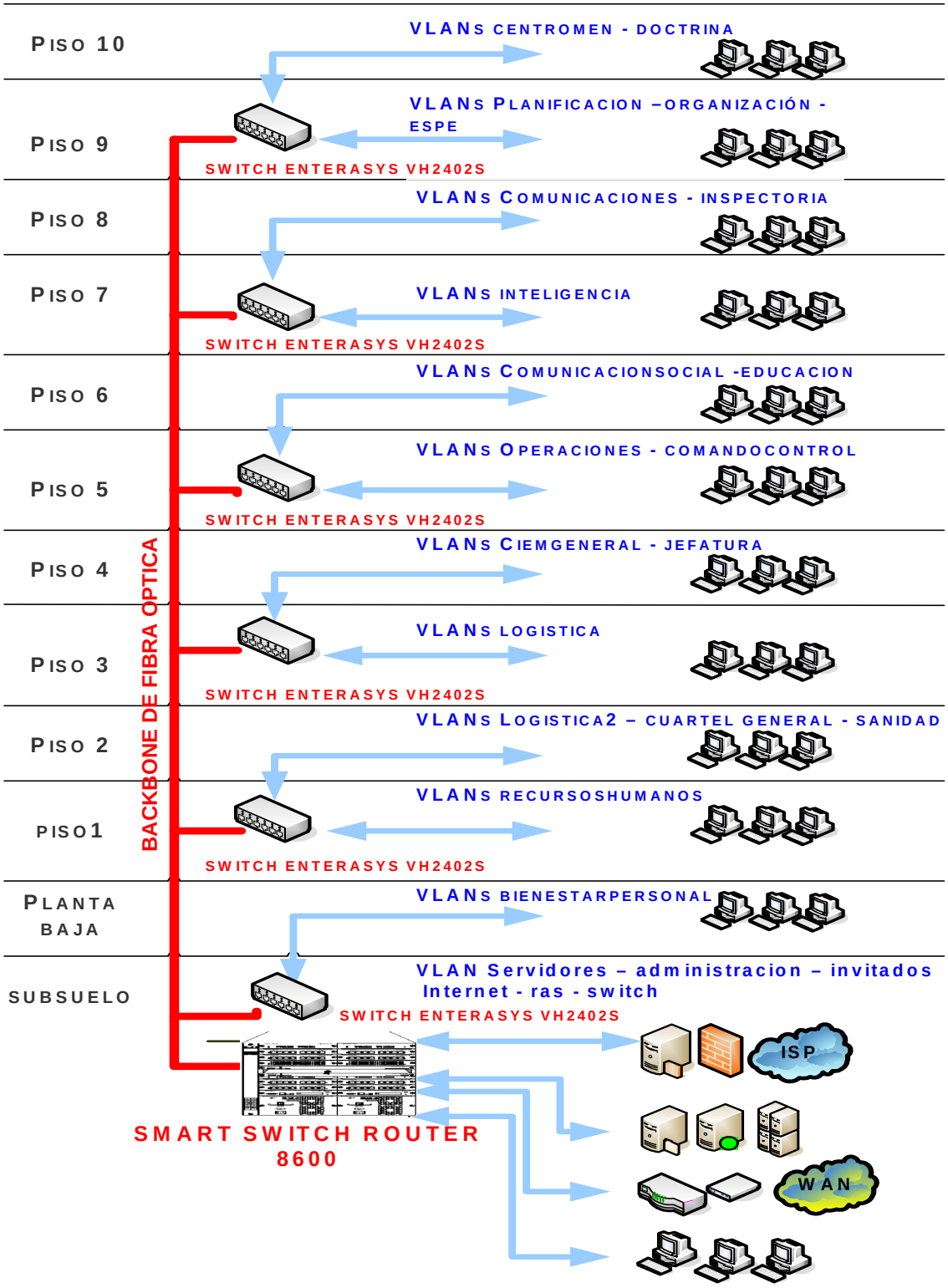


Figura 3.2: Diagrama físico de la creación de VLANS en la CGFT

3.3 DETERMINACIÓN DE LOS COMPONENTES NECESARIOS PARA LA CREACIÓN DE VLANs

Para el diseño propuesto y la reutilización los recursos existentes en la CGFT se necesitan los siguientes equipos activos:

- **1 SMART SWITCH ROUTER 8600 (SSR)**
  - 7 módulos de F.O. 1000 Base SX
  - 1 modulo de 10/100Base-TX de 16 puertos

- **13 Vertical Horizon – Patch Release VH-2402S Enterasys VH2402S 24 puertos**

Se a tratado de unificar los equipos activos, (un mismo fabricante), que van a formar parte en el diseño, por motivos de mejorar la eficiencia y rendimiento de la Red informática, debido a que cuando existe una implementación con distintos fabricantes de los equipos activos no se puede aprovechar al máximo el rendimiento de ellos.

En el **ANEXO D (DESCRIPCION DETALLADA DE VLAN CGFT)** se describen en detalle la distribución de los usuarios en cada una de las VLANs propuestas, los puertos que ocupan, la cantidad de equipos activos que se necesita en cada piso (switches) y las direcciones IP que se les asignara a cada VLAN propuesta.

3.4 DESCRIPCIÓN DE HARDWARE Y SOFTWARE

A continuación se describirá las especificaciones técnicas dadas por el fabricante de los equipos activos con que se cuenta en la CGFT y que se utilizarán en el diseño propuesto.

3.4.1 SMART SWITCH ROUTER 8600 (SSR)

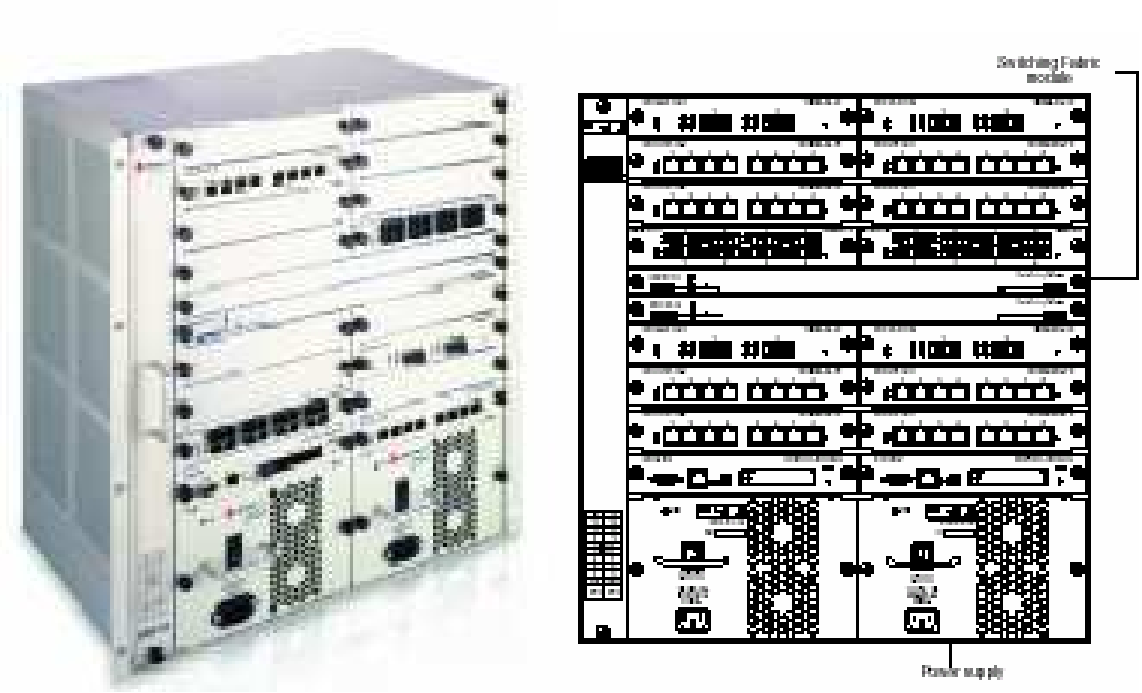


Figura 3.3: SSR 8600

CARACTERISTICA	DESCRIPCION
Throughput	• 32-Gbps non-blocking switching fabric. • Permite el ruteo de 30 millones de paquetes por Segundo a través del throughput.
Capacidad	• 250,000 rutas • 4,000,000 flujos de aplicaciones en la capa 4 • 800,000 direcciones MAC en capa 2 • 4,096 LANs Virtual (VLANs) • 20,000 filtros de control acceso y seguridad en capa 2 • MB de buffering de entrada/salida por cada puerto Gigabit • 1 MB de buffering de entrada/salida por cada puerto 10/100

	• 20 MB de buffering compartido de entrada/salida por cada puerto WAN en el modulo WAN • 32 MB de buffering de entrada/salida por cada paquete por el puerto SONET/SDH OC-3c • 64 MB de buffering de entrada/salida por cada paquete por el puerto SONET/SDH OC-12c
Ruteo de Protocolos	• IP: RIP v1/v2, OSPF, BGP 2, 3, 4 • IPX: RIP, SAP • Multicast: IGMP, DVMRP
Bridging and VLAN protocols	• 802.1d Spanning Tree • 802.1Q (VLAN trunking)
Protocolos de Interfase intermedios	• 802.3 (10Base-T) • 802.3u (100Base-TX, 100Base-FX) • 802.3x (1000Base-SX, 1000Base-LX) • 802.3z (1000Base-SX, 1000Base-LX)
Calidad de servicio (QoS)	• Priorización en capa 2 (802.1p) • Flujo de origen y destino en capa 3 • Flujo de origen y destino en capa 4 • Flujo de aplicaciones en capa 4
RMON	RMON v1/v2 por cada puerto
Administración	• SNMP • CoreWatch software (GUI) • Emacs-like Command Line Interface (CLI)

Monitoreo de puertos	• Trafico en el modulo de control • Trafico de puertos específicos. • Trafico de de específicos chassis slots (line cards)

Tabla 3.2: Especificaciones técnicas del SSR 8600

3.4.2 ENTERASYS VH2402S 24 PUERTOS

Figura 3.4: ENTERASYS VH2402S 24 PUERTOS

CARACTERISTICA	DESCRIPCION
Switching Bandwidth	16 Gbps
Forwarding Throughput	6.55 Mpps (single unit)/45.85 Mpps (7 high stack)

MAC Address Capacity	8.000
VLAN Capacity	255
Flash Memory	2 MB
DRAM	8 MB
Fuente de poder	Fuente de poder de AC
Alto rendimiento de conectividad	24 ports de 10/100 Mbps de alta velocidad de conectividad con la opción de aumentar 2 slots de expansión que puede ser usado para conexiones uplink para el centro de datos o la red vía 100Base-FX o 1000Base-X y además tiene un spot dedicado a la administración. Configuración de datos para tener una cola de prioridad de trafico, con la norma IEEE 802.1p Tabla de direcciones MAC de 8,000 MAC para integración de grandes empresas.
Stackable design	Permite hacer Stack con siete unidades dando un total de 168 puertos 10/100.

Simplicidad de administración	Administración vía red y vía puerto de consola local de configuración, web browser o SNMP-based network management, NetSight Se puede administrar una stack entero como una simple entidad vía un agente opcional de administración. IGMP identifica snooping y segregates unicast y multicast paquetes de trafico
Soporte Estándar de VLANs	Estándar de VLANs basado en la norma IEEE 802.1Q

Tabla 3.3: Especificaciones técnicas del Enterasys VH2402S

Mayores detalles técnicos se los puede observar en los **ANEXOS E** (SMART SWIRCH ROUTER SSR8600) **Y ANEXO F** (SWITCH ENTERASYS VH-2402S2)

3.4.3 SOFTWARE

No se necesita de software adicional porque se puede configurar estos equipos activos vía red y vía puerto de consola, teniendo instalado mínimo el Sistema Operativo Windows y se puede ingresar a estos equipos por la opción Hyper terminal.

También se puede configurar estos equipos vía Telnet

3.5 RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE LAS VLANS EN LA ORGANIZACIÓN

El procedimiento para la implementación de VLANs en la CGFT es un procedimiento que requiere de mucho cuidado y precaución debido a que la red informática se encuentra en plena producción. Es necesario establecer etapas o fases de actividades, las mismas que se puedan ejecutar progresivamente para no entorpecer el normal funcionamiento de la CGFT. Estos procedimientos que se han de realizar no deben poner en peligro la red informática y mucho menos causar daños graves al funcionamiento de la red, razón por la cual se recomienda la implementación en etapas.

Estas etapas son las siguientes:

- Notificación del proyecto
- Adecuación de la red informática y segmentación de la red.
- Creación de VLANs
- Pruebas y administración de las VLANs

3.5.1 NOTIFICACIÓN DEL PROYECTO

El primer paso que se debe realizar es notificar tanto al personal del centro de computo, usuarios que ocupan la red informática y todo personal involucrado con la administración, control, utilización y supervisión de la red informática del objetivo y alcance de la implementación de VLANs, los posibles problemas que pueden presentarse en el transcurso de la implementación y la actitud que deben tomar ante estos inconvenientes.

Esta notificación es muy necesaria para evitar que se produzca un caos o incertidumbre al no saber que esta sucediendo con la red informática cuando en algún momento no este en funcionamiento o no exista conexión entre usuarios,

servidores, servicios y el usuario comprenda que estos inconvenientes son por motivos de implementación de VLANs en la CGFT.

3.5.2 ADECUACIÓN DE LA RED INFORMÁTICA Y SEGMENTACIÓN DE LA RED.

Una vez cumplido la primera fase y con la información que se recopilo del capítulo anterior que es el inventario de todos los equipos activos que componen la red informática con su ubicación y usuarios que están conectados se debe proceder a realizar los cambios que fueren necesarios, esto es, creación, eliminación o reubicación de usuarios y servidores, siempre cumpliendo las normas de cableado estructurado. También se debe adecuar los cuartos de comunicaciones con equipo que se ve ha utilizar como son: switches, routers, hubs, etc.

Se debe disponer de los respaldos de las configuraciones anteriores de servidores y switches. Con la finalidad que si se comete algún error grave inmediatamente se pueda regresar a la anterior configuración y así evitar problemas con las actividades normales de la institución. Esto obliga a ejecutar un plan de contingencias que corresponda a la falla de cada equipo, servicio, aplicación, cableado, personal técnico y administrativo.

En esta fase también se debe cambiar si fuera necesario los hubs por switch, para la segmentación de la red, en el caso de estar utilizando hubs, Una vez sustituido los hubs por switch se debe realizar las respectivas pruebas de conectividad entre usuarios y servicios para evitar inconvenientes en la red informática y poder corregir a tiempo estos problemas.

Los cambios que se realizan deben tratarse de efectuar en horarios no laborables para no interrumpir el normal funcionamiento de la institución por ejemplo debería realizarse en horas de la noche.

3.5.3 CREACIÓN DE VLANS

Una vez segmentado la red se debe proceder a la creación de VLANs, para esto todo el personal que esta involucrado en este proyecto debe familiarizarse con las características de los equipos, su funcionamiento, ventajas, desventajas que presentan y saber como reaccionar ante cualquier inconveniente que se presente con los equipos utilizados en el proyecto.

Todas las VLANs creadas estarán documentadas con el mayor detalle posible y tener un plan de recuperación y prevención por escrito para omitir problemas en el futuro. El plan de recuperación, es un documento que posee todos los procedimientos a seguir en caso de un siniestro o fallas.

3.5.4 PRUEBAS Y ADMINISTRACIÓN DE LAS VLANS

Una vez realizado la configuración de las VLANs en los equipos activos de la red informática el paso final es realizar las respectivas pruebas con ayuda de de herramientas administrativas que se encuentran en el mercado.

Entre las diferentes pruebas que se deben realizar están:

- Monitoreo de tráfico de red para constatar las mejoras con la nueva implementación.
- Conectividad entre las subredes de la Institución.
- Monitoreo del ancho de banda.
- Monitoreo de protocolos que fluyen a través de la red informática

Todo cambio realizado y errores presentados en el transcurso de estas fases de implementación estarán debidamente documentados.

3.6 RECOMENDACIONES DE POLITICAS DE ADMINISTRACION Y SEGURIDAD EN LAS VLANS

El propósito de este proyecto no es establecer políticas de administración y seguridad de la red, lo único que se realizará es dar las recomendaciones de políticas de administración y seguridad en la red informática para la optimización y mejor administración de las VLANS con la finalidad de concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

Se recomendará la necesidad de crear una sección o unidad dentro de la CGFT destinada exclusivamente a la creación, implementación, control, modificación y actualización de estas políticas de administración y seguridad tomando en cuenta que es lo más importante que se quiere proteger es la operación y manejo de la información de la Institución.

Hablar de un sistema cien por cien seguro, es imposible porque el costo de la seguridad total es muy alto y puede ocasionar serios problemas en los bienes y servicios que presta la organización.

La solución es establecer Políticas de seguridad que son documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos tanto de usuarios como administradores. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. **"13"**

A continuación se indicaran donde se deben tomar medidas de prevención para mejorar la seguridad en la organización: **"14"**

1. Seguridad Lógica.
2. Seguridad en las Comunicaciones.
3. Seguridad de las Aplicaciones.
4. Seguridad Física.

5. Administración del Centro de Cómputos.
6. Auditorias y Revisiones.
7. Plan de Contingencia.

Se debe considerar de mucha importancia cada uno de estos puntos, pero el trabajo no esta orientado a crear políticas de seguridad, si no más bien a mencionar algunas de estas medidas que se deberían tomar en cuenta para mejorar la seguridad, así se tiene:

- Se debería establecer un procedimiento formal para la creación y eliminación de un usuario en el sistema.

- Cuando se crea un usuario se debe establecer permisos mínimos para realizar sus tareas y auditar a los mismos sobre operaciones y cambios que han realizado al sistema inclusive a los administradores y personal que realizan el mantenimiento y establecer horarios para la utilización de recursos computacionales.

- Se recomienda por seguridad que el administrador debería loggearse sólo desde las terminales que se encuentran en el centro de cómputo.

- El sistema deberá finalizar toda sesión interactiva cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de tiempo determinado y tener instalado un protector de pantalla con contraseña.

- Cuando se realice un mantenimiento externo, se debe crear una cuenta de usuario especial para estos fines y sólo con los permisos necesarios para realizar estas funciones utilizando protocolos y servicios de comunicación que garanticen la seguridad de los datos que se transmiten a través de la red.

- El password deben tener un conjunto de caracteres alfa-numérico, con una longitud mínima de caracteres que permita el sistema una máxima

seguridad y debe tener un tiempo de caducidad. Además este password no debe ser mostrada en pantalla y estos datos deben ser encriptados mientras son transmitidos a través de red al servidor.

- Toda la configuración física como lógica de la red debe ser documentada.

- Se debe disponer de más de un medio de transmisión en caso que falle el primer medio de transmisión.

- Se debe controlar el tráfico entrante y saliente de la red interna mediante dispositivos de seguridad por ejemplo firewall, Proxy.

- La CGFT debe disponer de un sistema de mail externo y uno interno, con diferentes dominios. De esta manera, las comunicaciones entre el personal de la empresa se realizarán sin exponer los mensajes a Internet.

- El administrador de mail no debe ser utilizado para enviar correo basura (SPAM) y los datos que se consideren confidenciales o críticos deben ser encriptados.

- Todos los equipos de la empresa debe poseer una herramienta antivirus ejecutándose permanentemente y en continua actualización como también disponer políticas y recursos que permitan restaurar los sistemas en caso de problemas causados por virus informáticos.

- Los servicios o protocolos que no se utilicen deben ser deshabitados para garantizar la seguridad en la institución.

- El sistema operativo que se tiene instalado en los servidores debe tener características como: alta confiabilidad, escalabilidad, performance, disponibilidad de software de aplicaciones, actualizaciones, compatibilidad e interoperatividad con los sistemas operativos de las PC´s, ser amigable con el usuario, disponibilidad de documentación entre otros requerimientos.

- El sistema operativo en lo que refiere a seguridad informática debe disponer de: identificación, autenticación, control de acceso, login, incorruptibilidad, fiabilidad, seguridad en la transmisión, backup de datos, encriptación, funciones para preservar la integridad de datos, etc.

- Los archivos y carpetas donde se encuentran almacenados datos y aplicaciones deben tener controles de acceso, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador.

- Se debe establecer un plan de migración en caso de cambios o actualizaciones en el sistema como también en las aplicaciones que usa.

- Se debe establecer estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red informática de todo esto se debe hacer un backup con la finalidad que cuando se realice cambios en la configuración de los servidores y exista un error grave se pueda disolver los cambios realizados.

- Se debe realizar chequeos periódicos en las PC´s, los servidores y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

- Se deben realizar pruebas del software desarrollado, con el fin de evitar inconvenientes al momento de estar en plena producción.

- Si se contrata terceros para el desarrollo de aplicaciones, Se debe exigir la aplicación ejecutable, código fuente de la aplicación, documentación del desarrollo, manual de uso como también los derechos de autor.

- Antes de realizar la compra de una aplicación de software, se debe analizar costo beneficio, adaptabilidad a los sistemas operativos, que medidas de seguridad tiene, entre otros requerimientos.

- El área del centro de cómputo en donde se encuentran los servidores, switches y demás equipamiento crítico debe ser restringido y solo debe ser permitido el acceso a los administradores y personal autorizado y disponer de una adecuada protección física y mantenimiento permanente.

- Se debe disponer de un generador de energía en caso de cortes de suministro eléctrico, y UPS en el centro de computo para que se apaguen de forma segura los servidores.

- El diseño del centro de cómputo debe ser proyectado para un crecimiento futuro y normas de cableado estructurado y así evitar complicaciones al momento de su expansión de su red informática.

- Se debe disponer de herramientas de monitoreo de red, que permitan medir periódicamente el nivel de interferencia, ancho de banda, con el fin de tomar las acciones correctivas necesarias y evitar ataques como denegación de servicio (DoS), problemas de sniffing, spoofing, etc.

- El centro de cómputo debe estar a cargo de profesionales que tengan experiencia en el manejo de los recursos informáticos como también en la seguridad informática.

- Se debe delegar a una persona o grupo de personas de la seguridad del sistema, coordinación de las tareas de políticas de seguridad, el cumplimiento de estas, planificación de actividades, desarrollo de planes de seguridad a corto y largo plazo entre otras responsabilidades.

- Se debe implementar mecanismos para la interacción entre usuarios y administrador del sistema para que puedan hacer llegar sus comentarios y sugerencias.

- Todo el personal del centro de cómputo como los usuarios deben ser capacitados continuamente en las tecnologías utilizadas en la organización.

- Se deberá generar una copia de respaldo de toda la documentación del centro de cómputo, incluyendo el hardware, el software, y el plan de contingencias, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

- Para la realización de auditorias y revisiones del sistema la CGFT debe tener las herramientas necesarias para garantizar un correcto control y auditabilidad.

- Se debe disponer de herramientas que registren, eventos respecto a los servidores: los servicios de mail, servicios de red, configuración de los servidores, utilización del CPU, reinicio de servidores y analicen estos registros generando alarmas de acuerdo a los eventos acontecidos y personal que analice estos eventos y tome decisiones correctivas.

- Con respecto al uso del Internet se debe almacenar información sobre: número IP de la máquina conectada, dirección de las páginas visitadas, cookies guardadas, archivos descargados, servicios utilizados, aplicaciones utilizadas, para una auditoria confiable y controlar el uso correcto a este servicio.

- Con respecto a la utilización del correo electrónico deben almacenarse datos sobre: correo entrante y saliente, hora de envío, contenido del mail, asunto del mail, archivos adjuntos, reporte de virus de cada parte del mail, direcciones de máquina destino y fuente, tamaño del mensaje.

- Con respecto a la utilización de la red informática deben almacenarse datos sobre: ancho de banda utilizado y cuellos de botella en el tráfico de red, tráfico generado por las aplicaciones, recursos de los servidores que

utilizan las aplicaciones, el estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta), intentos de intrusión, uso de los protocolos, solicitudes de impresión de datos de la empresa.

- Se debe generar procedimientos, manuales de respaldo para cada una de las actividades desarrolladas en la empresa. También se debe preparar, probar y mantener actualizado un plan de contingencias. Dicho plan deberá ser desarrollado de forma tal que cubra las distintas áreas de riesgo.

- El equipamiento informático de la empresa debe contar con dispositivos de respaldo, ante cualquier tipo de incidente.

- Se debe asignar un orden de importancia a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia.

3.7 TIEMPO APROXIMADO Y ANÁLISIS DE COSTOS PARA LA IMPLEMENTACIÓN DEL PROYECTO EN LA CGFT

3.7.1 TIEMPO APROXIMADO

Una aproximación del tiempo estimado en la implementación de las VLANs en la CGFT se describe en la siguiente tabla tomando en cuenta que la red ya se encuentra en producción por lo que hay que realizar cambios puntuales en determinadas Direcciones y Departamentos.

ACTIVIDAD	TIEMPO ESTIMADO EN DIAS LABORABLES			
Notificación del proyecto	**15**			
Adecuación de la red informática y segmentación de la red		**30**		
Creación de VLANs			**10**	
Pruebas y administración de las VLANs				**PERMANENTE**

Tabla 3.4: Tiempo aproximado de implementación de VLANs en la CGFT

3.7.2 ANALISIS DE COSTOS

A continuación se realizará el análisis de costos referente a instalaciones de ser necesarias, en caso de requerirse adicionar estaciones de trabajo. Por esta razón se ha considerado los costos de red de datos, red eléctrica, equipos activos de red, costos por servicios profesionales por concepto de configuración, diseño y capacitación El objetivo de este análisis, es determinar la cantidad de recursos económicos necesarios para el futuro crecimiento de la red de datos,

Nuevos puntos de red de datos.

ITEM	DESCRIPCION	CANTIDAD	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
A	INSTALACIÓN DE PUNTOS DE CABLEADO ESTRUCTURADO CAT 6	1	70.00	70.00
	1 PUNTOS DE DATOS			
	Materiales a utilizarse de acuerdo a la necesidad:			
	Metros de Cable UTP CAT 6			
	Patch cords de 3 pies desde el patch panel hasta el switch			
	Patch cords de 7 pies desde los face plates a los equipos			
	Cajas sobrepuestas, Jacks			
	Instalación de canaleta vista con división y accesorios			
	Mano de obra, Certificación de puntos, Etiquetación			
VALOR TOTAL POR CADA PUNTO DE DATOS				**70.00**

Tabla 3.5: Costos de Cableado Estructurado

Nuevas instalaciones eléctricas bajo ups.

ITEM	DESCRIPCION	CANTIDAD	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
1	INSTALACION DE PUNTOS DE ELECTRICOS UPS	1	38.00	38.00
	Materiales a utilizarse de acuerdo a la necesidad:			
	Metros de Cable eléctrico flexible #12			
	Tomacorrientes eléctricos polarizados			
	Etiquetación y pruebas			
	Instalación de canaleta vista con división			
	Realizado bajo normas NEC e IEEE			
VALOR TOTAL POR CADA PUNTO ELECTRICO				**38.00**

Tabla 3.6: Costos de tomas eléctricas reguladas UPS

Para realizar el análisis de costos de los elementos activos de comunicación de la red, se consideró las características de los equipos que se detalla en el **anexo** E (Switch Enterasys VH2402S2), además se recomienda tener un stock de 2 equipos para los pisos, mismos que servirán para contingencia y pruebas.

ITEM	DESCRIPCION	CANTIDAD	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
A	Switch de 24 puertos Capa 3	3	2100.00	6300.00
VALOR TOTAL EN EQUIPOS ACTIVOS PARA LOS PISOS				6300.00

Tabla 3.7: Costos de Equipos activos para los pisos

Costos referenciales de un profesional experto en redes de acuerdo al mercado nacional vigente

ITEM	DESCRIPCION	CANTIDAD (HORA/TECNICA)	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
A	El proyecto de aplicación de VLANs comprende las siguientes etapas.			
A.1	Definición de solución VLAN a aplicarse y esquema lógico de la misma.	20	20.00	400.00
A.2	Servicio profesional de Diseño y Configuración de VLANs en los equipos activos (13 switches y 1 router Enterasys) existentes al momento	24	80.00	1920.00
A.3	Pruebas de conectividad a nivel de capa 2 y capa 3	8	20.00	160.00
A.4	Capacitación del personal del área de comunicaciones para configurar, mantener y administrar la solución establecida	10	20.00	200.00
A5	Apoyo para la elaboración de la documentación que registre la solución y sirva de instructivo para los procedimientos de modificación, administración y control de la red LAN	10	20.00	200.00
VALOR TOTAL POR SERVICIOS PROFESIONALES				2880.00

Tabla 3.8: Costos por servicios profesionales

CAPÍTULO IV

IMPLEMENTACIÓN DE UN ESQUEMA PROTOTIPO

4.1 INTRODUCCION

En este capítulo se implementa un prototipo el cual especificará básicamente como se configura una parte de las VLANs en el edificio de la CGFT, tomando en cuenta que el diseño que se propuso es escalable facilitando de este modo la creación de más VLANs en el futuro de acuerdo a las necesidades de la CGFT.

También se especificara los pasos a seguir para la implementación de VLANs en la CGFT tomando en cuenta la reutilización de sus equipos que actualmente dispone, tratando de que la inversión económica que se destine para este proyecto sea lo menos impactante para la institución.

4.2 EQUIPOS USADOS EN LA IMPLEMENTACION DEL PROTOTIPO

A continuación se describen los equipos activos que se utilizaron para la creación de las VLANs en la CGFT.

- SMART SWITCH ROUTER 8600 (SSR), es la parte principal porque cumple la función de permitir o negar el acceso de los usuarios a los diferentes servicios controlando, ruteando y comunicando entre las diferentes VLANs toda esta función lo realiza en la capa 3 del modelo OSI y utilizando el estándar (802.1q).

- Switches de piso horizontal ENTERASYS VH2402S 24 PUERTOS VH2402S, de 24 puertos UTP y un puerto de alta velocidad Gigabit para los enlaces de fibra óptica. cumpliendo la función de encapsular el tráfico (802.1q) de acuerdo a la VLAN de la que forma parte el usuario. El encapsulamiento (802.1q) es enviado por el backbone Gigabit Ethernet para que el SSR 8600 aplique los filtros y seguridades que corresponde a cada VLAN creada.

- Estación que desempeña las funciones de consola la misma que debe tener instalado cualquier sistema operativo, de preferencia Windows y un navegador de Internet, las características mínimas requeridas de preferencia en hardware deben ser, procesador Pentium III, con 256 en memoria RAM, un disco duro de 40 GB, tarjeta de red 10/100 Kbps con conector RJ45.

4.3 ESQUEMA DE DIRECCIONES IP Y ESQUEMA FISICO DEL PROTOTIPO

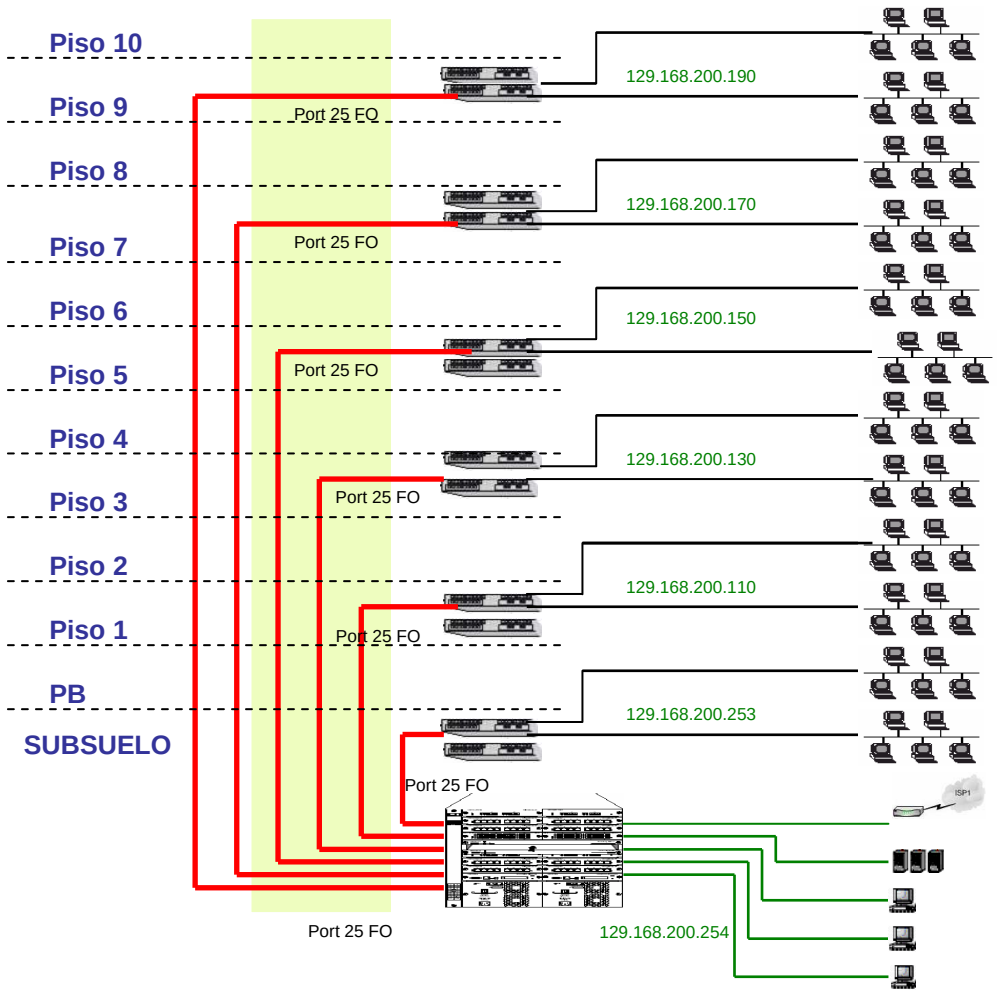
El esquema de direcciones IP interno asignado a la infraestructura se basa en el estándar de direcciones privadas RFC 1597, por motivos de sencillez se han seleccionado direcciones de clase C.
El esquema propuesto de direcciones de la arquitectura interna es el siguiente.

Red	192.168.X.0
Mascara de red	255.255.255.0
Puerta de enlace	192.168.X.253
Dirección difusión	192.168.X.255

Tabla 4.1: Esquema general propuesto de direcciones IP para la CGFT

Donde X se refiere a cada red VLAN, 101 VLAN 1, 102 VLAN 2, 113 VLAN 13, 200 VLAN switches.

La **Figura 4.1** especifica la ubicación de los switches ENTERASYS VH2402S en los pisos, las direcciones IP que tienen cada VLANs que se va a crear, su ID, que puertos utilizan para el Backbone entre el switch Enterasys VH2402S y el SMART SWITCH ROUTER 8600. Mayores detalles se puede observar en el **ANEXO E** (SMART SWITCH ROUTER SSR 8600).



NOTAS:

PISO 10: ID VLAN 101: 192.168.101.254 CENTROMEN
PISO 10: ID VLAN 102: 192.168.102.254 DOCTRINA
PISO 9: ID VLAN 103: 192.168.103.254 PLANIFICACION
PISO 9: ID VLAN 105: 192.168.105.254 ORGANIZACIÓN
PISO 9: ID VLAN 106: 192.168.106.254 ESPE
PISO 8: ID VLAN 107: 192.168.107.254 COMUNICACIONES
PISO 8: ID VLAN 108: 192.168.108.254 INSPECTORIA
PISO 7: ID VLAN 109: 192.168.109.254 INTELIGENCIA
PISO 6: ID VLAN 110: 192.168.110.254 COMUNICACIONSOCIAL
PISO 6: ID VLAN 111: 192.168.111.254 EDUCACION
PISO 5: ID VLAN 112: 192.168.112.254 OPERACIONES
PISO 5: ID VLAN 113: 192.168.113.254 COMANDOCONTROL
PISO 4: ID VLAN 114: 192.168.114.254 CIEMGENERAL
PISO 4: ID VLAN 115: 192.168.115.254 JEFATURA
PISO 3: ID VLAN 116: 192.168.116.254 LOGISTICA
PISO 2: ID VLAN 118: 192.168.118.254 LOGISTICA2
PISO 2: ID VLAN 119: 192.168.119.254 CUARTELGENERAL
PISO 2: ID VLAN 120: 192.168.120.254 SANIDAD
PISO 1: ID VLAN 122: 192.168.122.254 RECURSOSHUMANOS
PB: ID VLAN 123: 192.168.123.254 EDUCACION
SUBS: ID VLAN 125: 192.168.125.254 SERVIDORES
SUBS: ID VLAN 126: 192.168.126.254 ADMINISTRACION
SUBS: ID VLAN 127: 192.168.127.254 INVITADOS
SUBS: ID VLAN 128: 192.168.128.254 INTERNET
SUBS: ID VLAN 129: 192.168.129.254 RAS
SUBS: ID VLAN 130: 192.168.130.254 TEMPORAL
SUBS: ID VLAN 200: 192.168.200.1 SWITCH

Figura 4.1: Diagrama Físico

4.4 CONFIGURACIONES EN EL ENTERASYS VH2402S Y EN EL SMART SWITCH ROUTER 8600

4.4.1 CONFIGURACIONES BASICAS EN EL ENTERASYS VH2402S

El procedimiento básico que debe saber todo personal que utiliza estos equipos es el siguiente:

1. Ingresar al switch, poniendo su dirección IP en el browser
2. Configurar Máscara
3. Configurar el Getway de ser necesario
4. Ingresar al menú VLANs, definir las VLANs y se asignar puertos
5. Activar encapsulamiento 802.1Q

4.4.1.1 Guía para acceder a los SWITCHES ENTERASYS VH2402S

Para ingresar al switch, se lo puede hacer de dos maneras:

- Administrador, para realizar modificaciones en la configuración
- Invitado, para visualizar las configuraciones actuales

Paso 1:
Para ingresar como administrador se debe primero verificar si esta en la mismo subred a la que pertenece el switch.

Paso 2:
Una vez verificada la extensión, ingresar al switch, existiendo dos formas de ingresar: en modo browser o en modo menú (comandos).

Paso 3:

Para ingresar en modo browser, se debe digitar lo siguiente en el explorador: http://192.168.200.# SWITCH,

192.168.200. 254 PISO SUBSUELO
192.168.200. 253 PISO SUBSUELO
192.168.200. 110 PISO 1 Y 2
192.168.200. 130 PISO 3 Y 4
192.168.200. 150 PISO 5 Y 6
192.168.200. 170 PISO 7 Y 8
192.168.200. 190 PISO 9 Y 10

Paso 4:

Aparece una ventaja de dialogo, en la que se debe poner el nombre de usuario (por defecto Admin) y la contraseña (Según el piso en el que este ubicado el switch).

Figura 4.2: Autentificación de usuario para ingresar al Switch Enterasys

Paso 5:

Aparece una página Web, con todas las opciones de configuración del switch, en la parte superior, se muestran los puertos, que están conectados con color verde, muestra además si tiene conexión con otro switch.

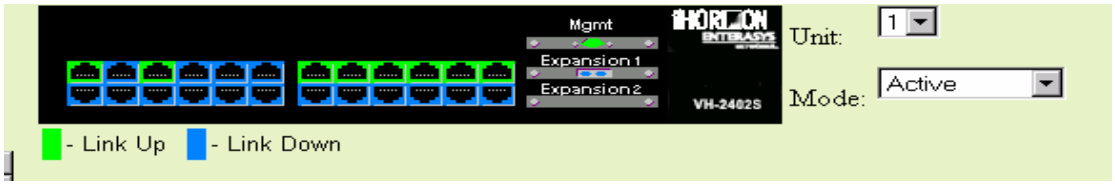


Figura 4.3: Visualización de estado de puertos y enlace

Paso 6:

En la parte izquierda de la página se muestra un menú donde esta la información general, y las opciones para la configuración.

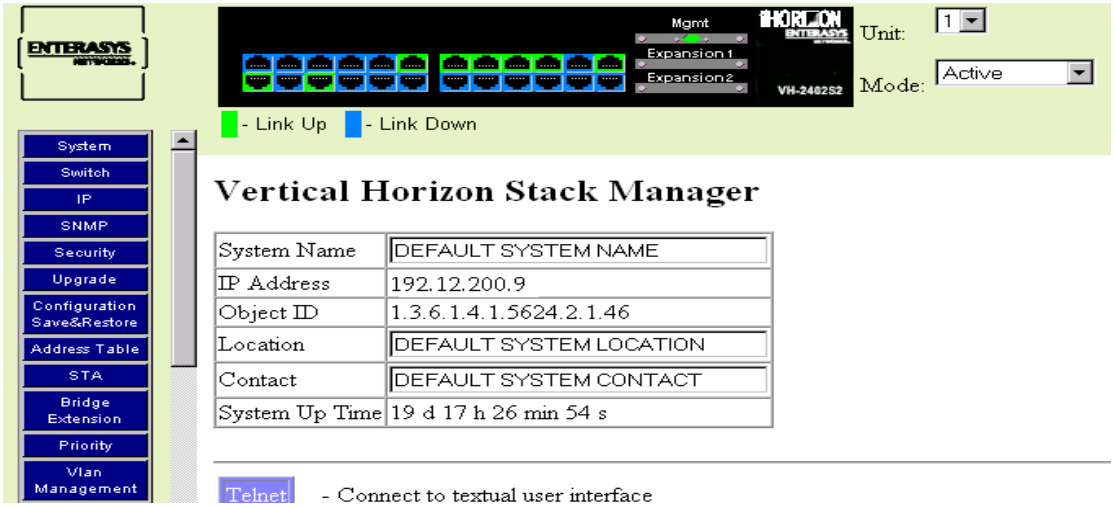


Figura 4.4: Menú de configuración del Switch Enterasys VH2402S

Paso 7:

Con la opción **Switch Information** se puede observar información correspondiente al equipo.

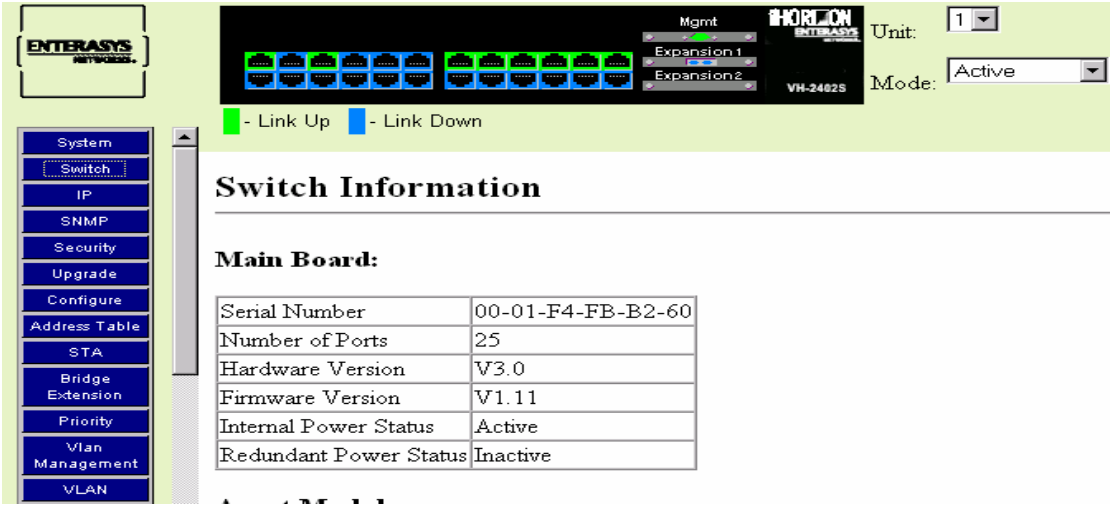


Figura 4.5: Visualización de información general del Switch Enterasys

Paso 8:

Para la configuración de la dirección IP del switch:

- Seleccionar **IP Configuración** en el menú de opciones
- En la opción **IP Address** se pone la dirección deseada, como se muestra en la figura 4.5
- En la opción **Subset Mask** se pone la mascara
- Se pone la Mac Address, y si fuera necesario o si tuviera el gateway

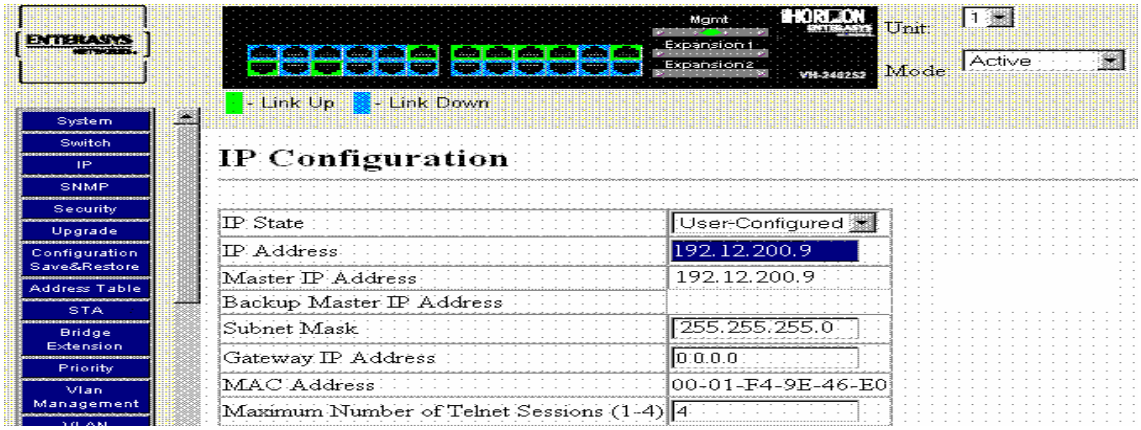


Figura 4.6: Configuración de direcciones IP en Switch Enterasys VH2402S

Paso 9:

Para cambiar el password del switch:

- Elegir la opción **Security**
- En la parte derecha se muestra una pantalla con tres opciones:
    - Password viejo
    - Password nuevo
    - Confirmar password

Una vez ingresados estos datos, dar clic en ***apply*** para guardar los cambios realizados.

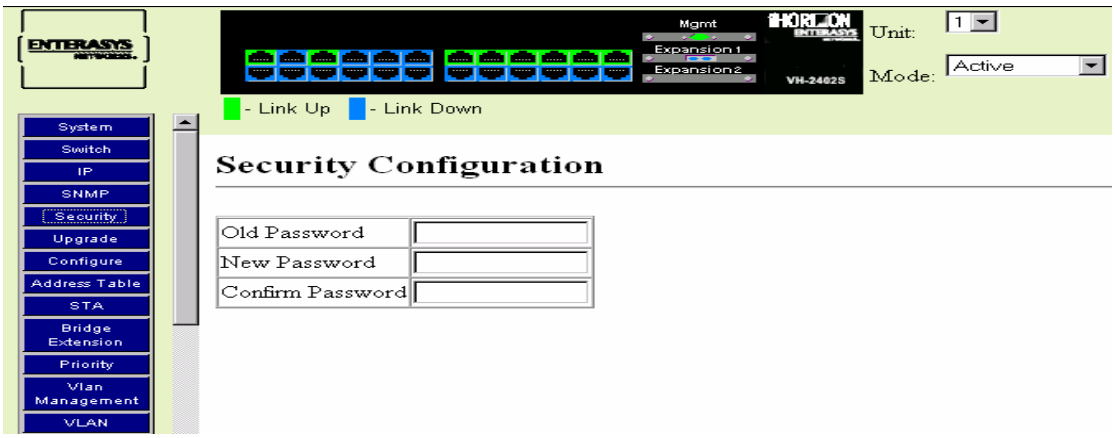


Figura 4.7: Configuración de claves de acceso

Paso 10:

Para la configuración de seguridades de puertos escoger la opción Port, dentro de esta aparece una opción **Port Security Configuration,** y seguir las siguientes instrucciones:

- Escoger el puerto
- El estado el cual debe ser estático, para que sea un puerto seguro
- Se debe poner la Mac Address de la máquina que se desea que acceda al Internet o esta conectada en la Intranet en ese puerto.
- Para agregar a la lista se escoge la opción ***add***.

- Para guardar los cambios se da clic en ***apply***

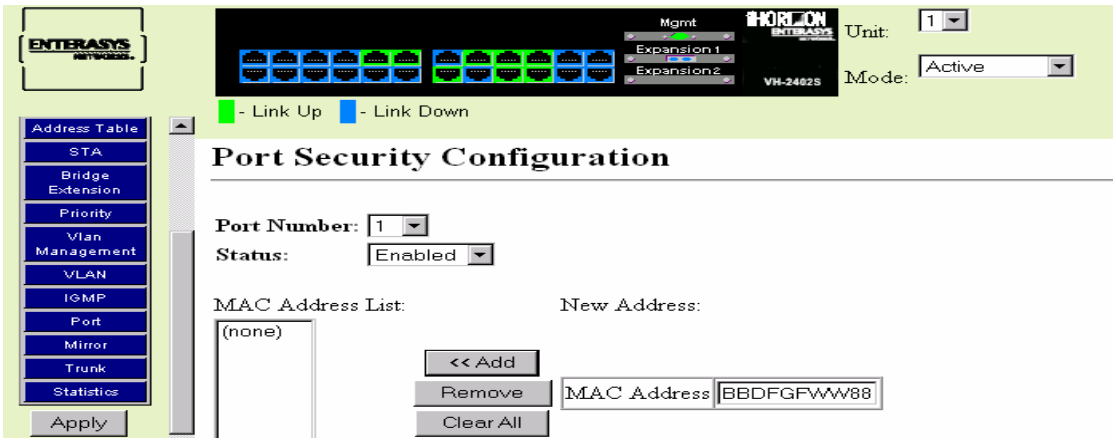


Figura 4.8: Configuración de seguridades por puertos

Todas estas configuraciones se las puede realizar siempre y cuando tenga permiso de administrador, de lo contrario se puede acceder al switch únicamente como invitado, es decir no se podrá realizar cambios, sólo visualizar la información del switch, el procedimiento descrito anteriormente es aplicable al resto de switch, ya que son del mismo modelo y fabricante.

A continuación la tabla 4.1 resume las ips y claves de acceso a los switch enterasys.

PISO N°	DIRECCION IP	MARCA	USERNAME	PASSWORD
SUBSUELO	192.168.200.253	ENTERASYS VH2402S 24 PUERTOS	admin	adminpb
PISO 1	192.168.200.110	ENTERASYS VH2402S 24 PUERTOS	admin	adminp1
PISO 3	192.168.200.130	ENTERASYS VH2402S 24 PUERTOS	admin	adminp3
PISO 5	192.168.200.150	ENTERASYS VH2402S 24 PUERTOS	admin	adminp5
PISO 7	192.168.200.170	ENTERASYS VH2402S 24 PUERTOS	admin	adminp7
PISO 9	192.168.200.190	ENTERASYS VH2402S 24 PUERTOS	admin	adminp9

Tabla 4.2: Usuario y claves de acceso a Switch Enterasys VH2402S

4.4.1.2 Procedimientos a seguirse para configurar y crear VLANs en el Router SSR 8600

Se propone una secuencia de pasos a seguir, los que guiarán, sobre como trabajar con los archivos de configuración del Ruter Enterasys VH2402S 24 puertos X - Pedition 8600.

Para poder tener una visión del diseño de las VLANs a crearse, se debe previamente diseñar el esquema lógico, y físico, en estos se debe tener recopilada la siguiente información:

- Direcciones IP de las VLANs
- ID para identificar las VLANs
- Nombre de la VLANs
- Puertos asignados a cada VLAN.

Guía a seguir para la creación de las VLANs en el Router SSR 8600:

1. Crear las VLANs en cada uno de los switch de piso según los usuarios, se sigue el procedimiento anteriormente descrito para los Switches Enterasys VH2402S.
2. Crear los puertos TRUNK EN EL ROUTER SSR 8600
3. Crear las VLANs en el Router SSR 8600:
4. Asignación de VLANS que pasan por el TRUNK en el Router SSR 8600 ejemplo; VLAN add port gi.6.2. to INTERNET
5. Asignación de puertos a las VLANs creadas.
6. Creación de interfaces y asignación de direcciones Ip a las VLANs creadas.
7. Permisos de acceso para las VLANs (acl)

4.4.2 Descripción de los comandos utilizados en el SSR 8600

Se refiere el procedimiento para ingresar al router SSR 8600 y los comandos usados en su configuración.

El ingreso al ruteador SSR 8600, se lo puede hacer de dos maneras, vía puerto de consola, a través de un conector serial de 9 pines, o vía red desde una estación que debe estar en la misma red que el ruteador, se debe usar el comando, telnet <ip del ruteador>, posteriormente solicitara la clave de validación para permitir el ingreso, a la consola.

Se proporciona información acerca de los comandos del SSR 8600 en el modo terminal de Interfase de línea de comandos (CLI), usado para configurar y administrar el ruteador SSR 8600, CLI agrupa los comandos por subsistemas, ejemplo para el uso del comando ip se lo debe combinar con otros comandos asi: ip set; ip show; ip configure.

EL CLI proporciona acceso a cuatro diferentes modos de comandos, cada modo de comandos provee un grupo de órdenes relacionadas, los modos de comandos son:

- User mode
- Enable mode
- Configure mode
- Boot PROM mode.

4.4.2.1 User mode

Después de logoniarse en el router SSR 8600, automáticamente se ingresa en User mode, los comandos disponibles en este modo es un subset de los que están disponibles en Enable mode, estos comandos permiten ver información básica del router y ejecutar herramientas elementales, ejemplo ping.

Prompt que muestra por default en User mode

```
xp>
```

4.4.2.2 Enable mode

Enable mode provee mas facilidades que en User mode, permite desplegar configuraciones críticas, incluidas las configuraciones del router, access control list (acl), y estadísticas SNMP.

Para acceder a Enable mode desde el User mode, se ingresa el comando <enable> o su abreviatura <en>, seguido solicita el ingreso de la clave para habilitar la consola de Enable mode.

Prompt que indica que se a ingresado en Enable mode.

```
xp#
```

4.4.2.3 Configure mode

Configure mode proporciona la capacidad, para configurar todas las características y funciones en el router SSR 8600, estas incluyen configuraciones de ruteo, acess control list (acl = listas de control de acceso) y spanning tree. Para ingresar en Configure mode se ingresa el comando <config> desde la consola Enable mode.

Prompt que indica que se a ingresado en Configure mode.

```
xp(configure)#
```

Cuando se esta en Configure o Enable mode se usa el comando <exit> y se presiona <enter> o se presiona Ctrl+Z para salir al previo modo de acceso.

4.4.2.4 Boot PROM mode

Si el router SSR 8600 no encuentra un imagen de un sistema valido en la tarjeta flash PCMCIA, el sistema puede ingresar programando el PROM mode. Si el sistema esta en PROM mode, se debe reiniciar el router, ingresando el comando <reboot> en el prompt de PROM boot.

4.4.2.5 Modos Native y Common CLI

El router SSR 8600 soporta dos interfaces estándar, el Native CLI y el Common CLI. Cada modo contiene comandos específicos que son accesibles solo desde dentro de cada modo en particular.

Para cambiar entre los dos modos. Se ingresa uno de los siguientes comandos.

4.4.2.5.1 Native a common

xp>cli set common

4.4.2.5.2 Common a Native

xp>terminal cli native

4.4.2.6 Comandos usados en la configuración de VLANs en el SSR 8600

A continuación se describe brevemente los comandos mas usados en la configuración de las VLANs.

Para crear una VLAN basado en puerto o protocolo, se debe ingresar el siguiente comando en modo de configuración.

Crear una VLAN	**vlan create** <vlan-name><type>**[id< num>]**

Para agregar un Puerto físico a la VLAN se ingresa el siguiente comando en modo de configuración.

Agregar puertos a la VLAN	**Vlan add port** <port list> **to** <vlan-name>

El comando vlan add ports agrega puertos y puertos trunk a una vlan existente.

Donde: <*port-list*>, son los puertos que se agregaran a la Vlan, se puede especificar un simple puerto o una lista de puertos, separadas por comas, ejemplo: et.1.3,et.(1-3).(4,6-8).

<*vlan-name*>, es el nombre de la Vlan a la que se esta agregando puertos

Para configurar un Trunk VLAN, se ingresa el siguiente comando en modo de configuración.

Configuración 801.1Q Vlan Trunk	**vlan make trunk-port** <port-list>

Configura los puertos especificados en trunk o puertos de acceso.

El comando vlan make convierte un puerto en una VLAN trunk o puerto de acceso de VLANs. Un puerto de VLAN trunk puede traficar multiples VLANs. Se usa puertos trunk cuando se quiere conectar juntos SSR con switches y envíar tráfico de multiples VLANs en un solo segmento de la red conectado a los switches. Cuando se crea un puerto trunk, se debe usar el comando vlan add ports y agregar los puertos tunk a la VLAN.

Cuando se crea un Puerto Trunk VLAN, se debe asegurar que el puerto a usarse no este ya asignado a una VLAN existente. Después de definir el trunk, se debe convertir a 802.1Q para agregarlo a una VLAN que no sea la de default.

Para configurar una interface, se ingresa el siguiente comando en modo de configuración.

Configura la interface IPv4	interface add ip <*InterfaceName*> address-netmask <*IPaddr-mask*> [peer-address <*IPaddr*>] [broadcast <*IPaddr*>]

El comando interface add ip, permite al usuario crear interfaces para, Ipv4.

El commando **interface add ip** configura direcciones secundarias para una IPV4 existente. Se usa este comando para configurar una dirección IPV4 y la mascara, la interface ya debe existir, para crear una interface se ingresa el comando **interface create ip.**

<*InterfaceName*> *Nombre de la interface* IPv4.

Para configurar un acl, se ingresa el siguiente comando en modo de configuración.

Crea un ACL IPV4	**acl** <*name*> **permit|deny ip** <*SrcAddr/Mask*> <*DstAddr/Mask*> <*SrcPort*> <*DstPort*> [<*tos*>] <*tos-mask*> **any [log]**

El comando acl permite crear ACLs (Listas de control de Acceso) y se puede aplicar para IPv4, IPv6, y IPX enterfaces en el SSR. Un ACL básicamente permite o niega cambiar paquetes con el criterio como es la dirección del paquete fuente y la dirección del destino, número de puerto TCP o UDP, y así sucesivamente. Cuando se aplica un ACL a una interface, se puede especificar si el ACL afecta tráfico entrante o el tráfico saliente.

Los comandos permit ip y deny ip definen una lista de control de acceso para permitir el bloqueo de trafico IPv4 de entrada o salida del router. La version IPv4 de el comando incluye protocolos basados en IP tales tcp, udp, icmp y igmp.

Para cada parámetro que describe un flujo, se puede especificar un valor o se puede usar la palabra any (Indica la condición "no cuida" = wildcard).

Cuando se especifica sólo algunos de los parámetros, los campos restantes requerirán la palabra any. Si no se especifica un valor para cualquier campo, el router SSR aplica una condición del wildcard, a cada campo y da el mismo efecto como si se hubiese especificado la palabra any.

Cuando se aplica un ACL a una interface, el router SSR, añade implícitamente una regla de negar a esa ACL, la regla de negación implícita negar todo tráfico.

<nombre> Nombre de la ACL. Usted puede usar un string de caracteres o un número, el string debe tener menos de 100 carácteres.

<SrcAddr/Mask> La dirección de origen y la máscara de filtro de este flujo. Si la dirección de origen es una red o una dirección de subred, se debe proporcionar el filtro de máscara. Generalmente, el filtro de máscara es la máscara de la red de esta red o subred. Si la dirección de origen es de un host entonces la mascara no se requiere. Por defecto, si una máscara no se proporciona, la dirección de origen es tratado como de un host. se puede especificar la máscara usando los tradicionales formatos de direcciones IP (“255.255.0.0”) o el formato CIDR (“/16”).

<DstAddr/Mask> La dirección del destino y la máscara de filtro de este flujo. Los mismos requisitos y restricciones para <SrcAddr/Mask> son aplicados a <DstAddr/Mask>.

<SrcPort> para TCP o UDP, el número del puerto de origen TCP o UDP. Este campo sólo aplica a tráfico TCP o UDP. Si el paquete entrante es ICMP u otro que no sea un paquete TCP o UDP y se especifica el origen y el puerto de destino, el router SSR 8600 no verifica el valor del puerto. El SSR 8600 verifica sólo la dirección ip del origen y destino IP en el paquete.

Se puede especificar un número de rangos de puertos usando símbolos del operador; por ejemplo, 10-20 (entre 10 y 20 incluido), >1024 (mayor que 1024), <1024 (menos de 1024) !=1024 (no igual a 1024). El número de puerto de algunos servicios populares ya se define como keywords.
Por ejemplo, para Telnet, se puede entrar por el puerto número 23 así como keywords de telnet

Los mismos requisitos y restricciones de <SrcPort> se aplican a <DstPort>.

<tos> Valor IP TOS (Tipo de Servicio). Se puede especificar un valor de TOS de 0 - 255.

<tos-máscara> El valor de la Máscara usado para el byte de TOS, el valor de la máscara puede ser de 0 - 255. El valor por defecto es 30.

Para configurar un **ip add route**, se ingresa el siguiente comando en modo de configuración.

Configurar una ruta estática	ip add route <*ipAddr-mask*>|**default gateway** <*hostname-or-IPaddr*> [host] [**interface** <*hostname-or-IPaddr*>] [**intf-list** <*IPaddr-list*>] [preference <*num*>] [**retain**] [**reject**] [**no-install**] [**blackhole**] [**gate-list** <*gateway list*>] [**unicast-rib**] [**multicast-rib**]

El commando ip add route crea una ruta estática y la ingresa en la tabla de ruteo. Esta ruta estática puede ser una ruta de default, una ruta a una red, una ruta a un host especifico.

<ip Addr-mask> Dirección y mascara IP de el destino. Se puede especificar la dirección y la mascara usando el formato tradicional (10.1.2.3/255.255.0.0) o el formato CIDR (10.1.2.3/16), si no especifica una mascara el router SSR 8600 usa la mascara natural para las direcciones, /8 para clase A, /16 para la clase B, /24 para la clase C.

gateway <*hostnameor-IPaddr*> La dirección IP o nombre de host para el siguiente salto al gateway.

[host]especifica que la ruta es la de un host

interface <*hostnameor-IPaddr*> la próxima interface de salto esta asociado con esta ruta.

Para configurar la información del sistema, hora y fecha, se ingresa el siguiente comando en Enable mode.

Configurar hora y fecha	System set date year <number> month <month-name> day <day> hour <hour> minute<minute> second<second>

Para configurar la información del sistema, tales como nombre, localización, contacto, se ingresa los siguientes comandos en modo de configuración.

nombre del sistema	system set name “<string>”
localización	system set location “<string>”
persona de contacto	system set contact “<string>”

Configuración de **Per-VLAN Spanning Tree con RTSP Enable**

El máximo número de per-VLAN spanning tree que puede soportar el SSR esta relacionada a la cantidad de memoria instalada en su sistema, Porque cada spanning tree asigna 1 MB de memoria, un sistema con 256 MB de memoria soportaría aproximadamente 200 per-VLAN spanning tree, de esto dependerá la cantidad de memoria necesaria con la que se debería configurar el hardware del router SSR.

Para la configuración del Spanning Tree se deberá seguir una secuencia de pasos como se indica en el siguiente ejemplo.

Para esto dos routers SSR 8600 serán conectados como se muestra en la Figura 4.9. Para esta conexión se creara una instancia per VLAN spanning tree con RTSP habilitado en el puerto gi.1.(1-2), et.3.1 en el SSR 1(XP1) y gi.2.(1-2) en el SSR 2 (XP2).

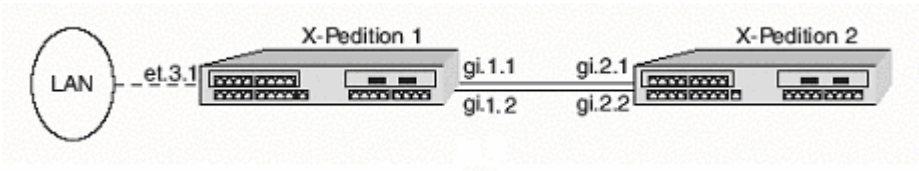


FIGURA 4.9: Ejemplo de configuración de SPANNING TREE

Primero, se creara una VLAN llamada MIVLAN, con VLAN ID 100 en ambos routers XP1 y XP2 y agregamos los puertos a la VLAN.

```
xp1(configure)# vlan create MIVLAN port-based id 100

xp1(configure)# vlan add port gi.1.(1-2),et.3.1 to MIVLAN
```

```
Xp2(configure)# vlan create MIVLAN port-based id 100

Xp2(configure)# vlan add port gi.2.(1-2), to MIVLAN
```

A continuación creamos una instancia de spanning tree para VLAN “MIVLAN”.

```
xp1(configure)# pvst create spaningtree vlan_name MIVLAN
```

```
Xp2(configure)# pvst create spaningtree vlan_name MIVLAN
```

Se debe habilitar PVST en gi.1.(1-2),et.3.1 en XP1 y gi.2.(1-2) en XP2

```
xp1(configure)# pvst  enable port gi.1.(1-2),et.3.1 spanning-tree MIVLAN
```

```
Xp2(configure)# pvst  enable port gi.2.(1-2) spanning-tree MIVLAN
```

Para habilitar RSTV para el spanning tree, se coloca la versión del protocolo a “rstp”.

```
xp1(configure)# pvst  set protocol-version rstp spanning-tree MIVLAN
```

```
Xp2(configure)# pvst  set protocol-version rstp spanning-tree MIVLAN
```

Para permitir una reconfiguración del segundo enlace, los enlaces entre gi.1.(1-2) en XP1 y gi.2.(1-2) en XP2 deberá ser los enlaces punto-a-punto. Se debería también definir et.3.1 en XP1 como un edge-port si este no es conectado a ningún otro edge que pueda generar lasos en la red

```
xp1(configure)# pvst  set port gi.1.(1-2) point to point Force Trae

xp1(configure)# pvst  set port et.3.1 edge-port True
```

```
Xp2(configure)# pvst  set port gi.2.(1-2) point to point Force True
```

4.4.3 CONFIGURACION DE VLAN EN SWITCH ENTERASYS VH2402S

Paso 1:

Ingresar al switch en modo browser.

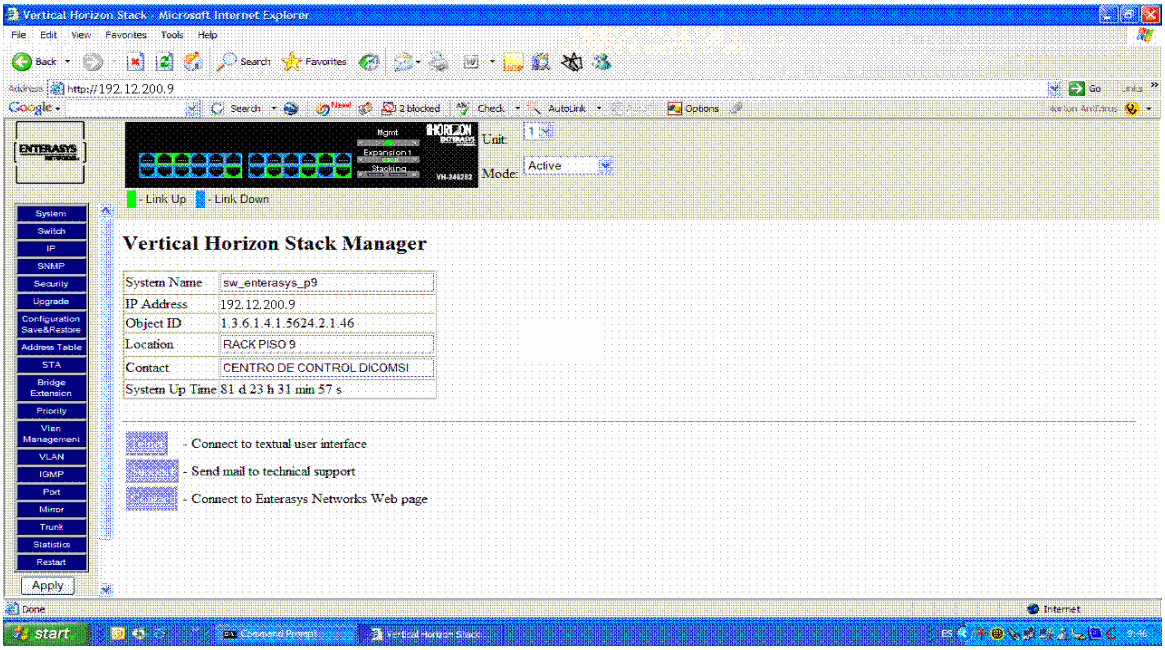


Figura 4.10: Configuración de claves de acceso

Paso 2:

Seleccionar VLAN Basic information, en donde se define la VLAN ID

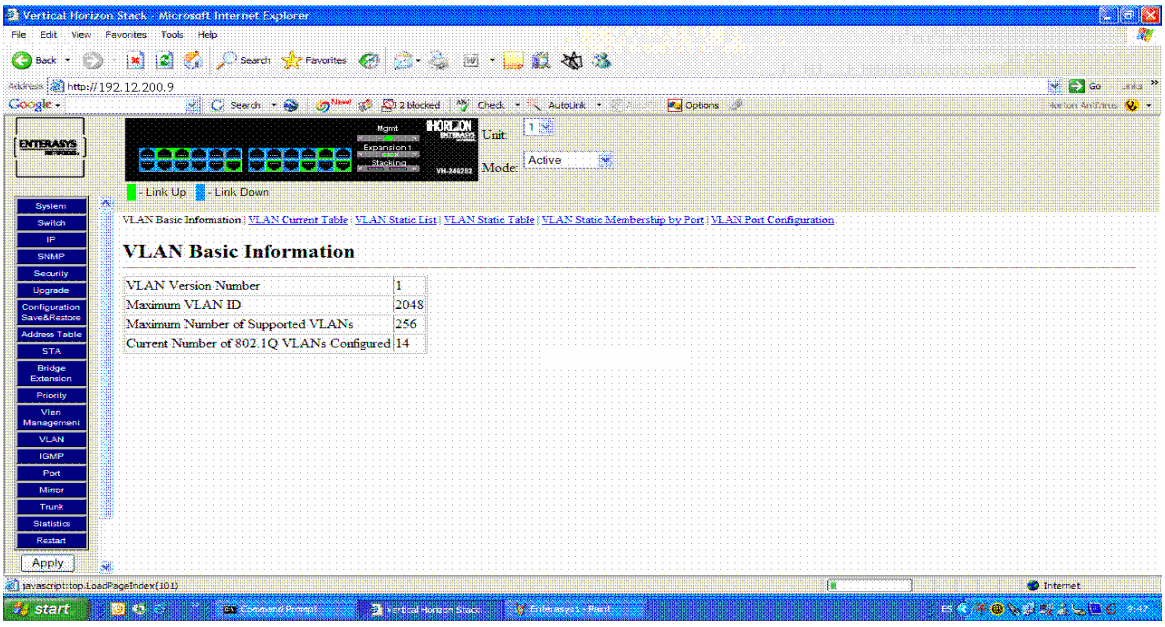


Figura 4.11: Identificación ID de la VLAN

Paso 3:

En la opción VLAN Current Table, encontramos información de cada VLAN y la asignación de puertos TRUNK, estos switches disponen de dos puertos para realizar el trunk , el puerto de fibra óptica que lo asigna como puerto 25, y el puerto 24 para un enlace con cable utp

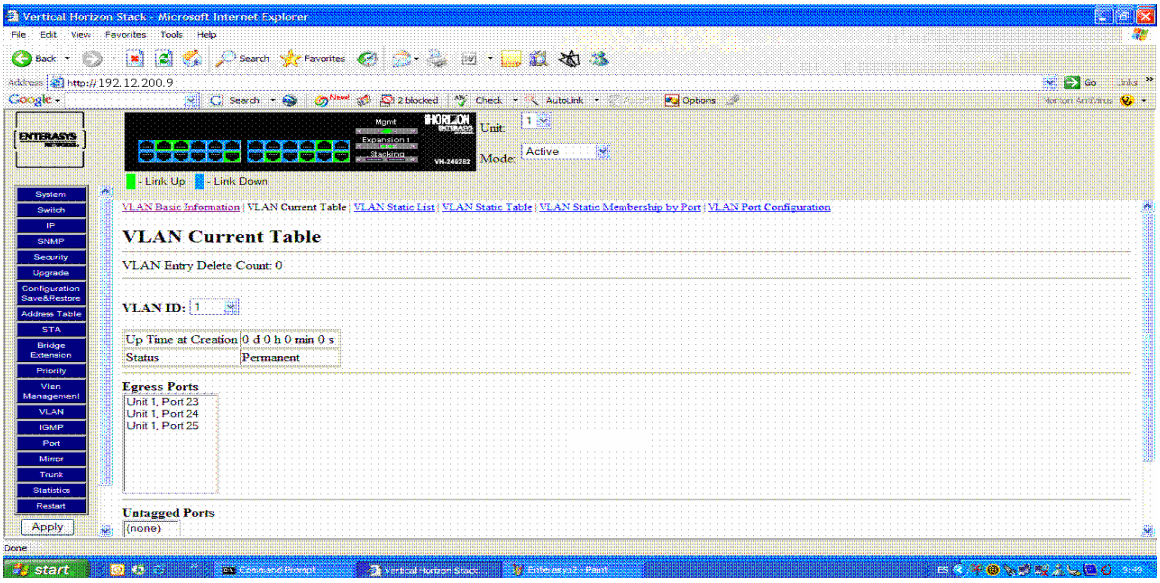


Figura 4.12: Asignación de puertos Trunk

Paso 4:

En la opción VLAN Static List, se observa las VLANS que se han configurado en el switch, y se puede crear nuevas VLANS

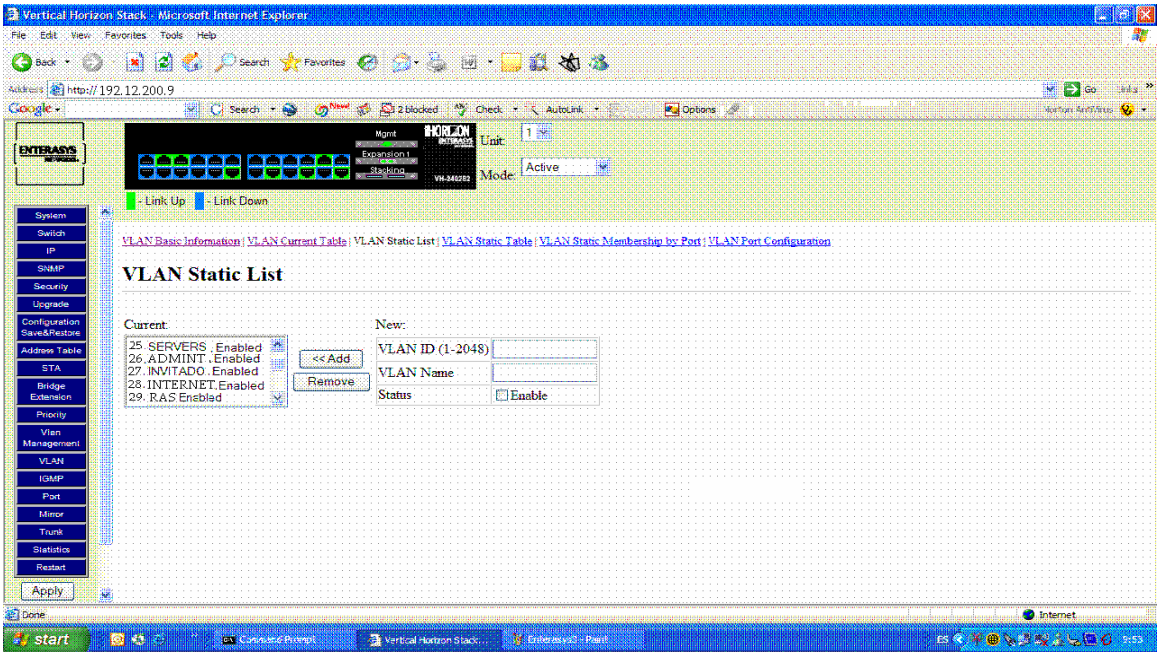


Figura 4.13: Creación de VLANs

Paso 5:

En La opción VLAN Static Table, se observa información de asignación de los puertos trunk.

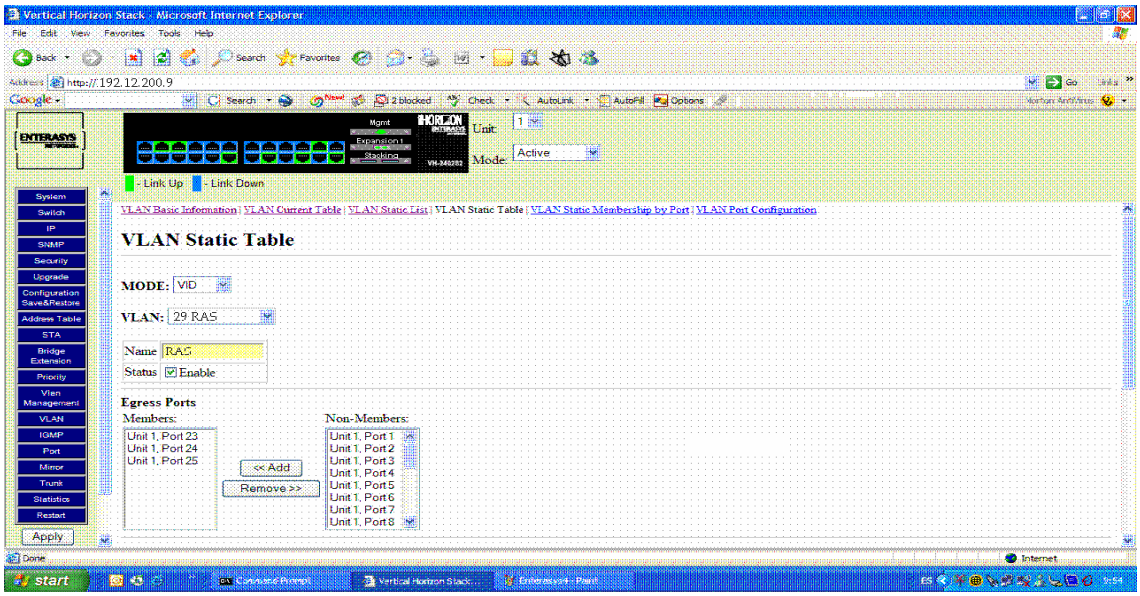


Figura 4.14: Asignación de Puertos Trunk

Paso 6:

Opción VLAN Static Menbership by Port, se asigna una VLAN creada a un puerto 22 (VLAN 6 ESPE usara los puertos 1, 2, 3, 5, 7, 22).

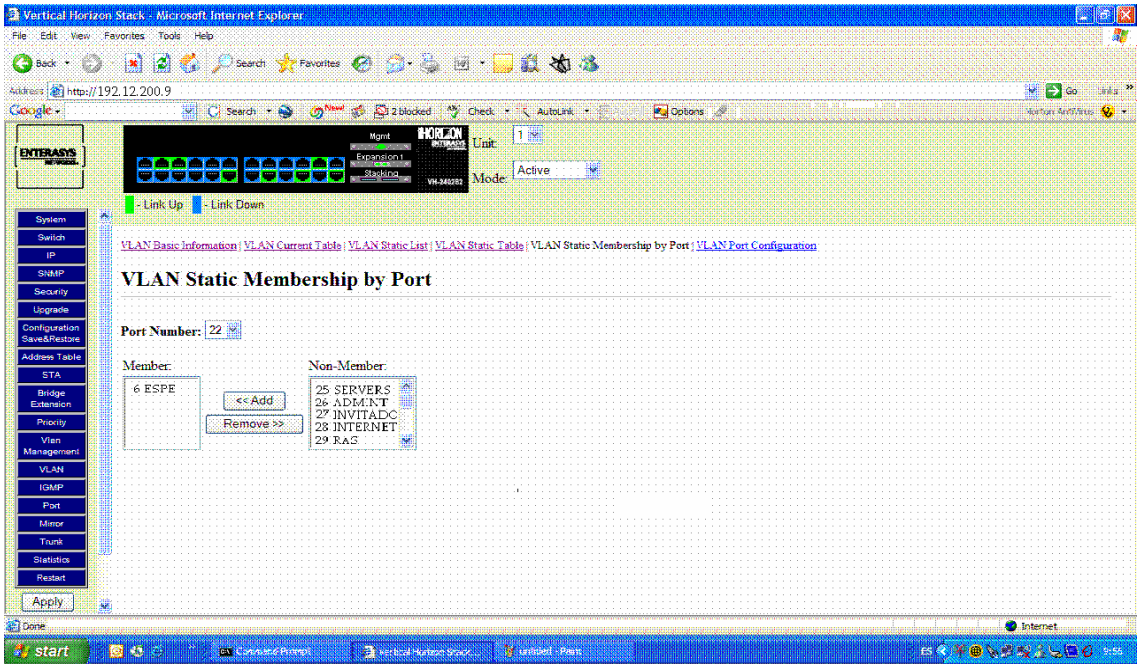


Figura 4.15: Asignación de puertos a una VLAN

Paso 7:

En opción, VLAN Port configuración, permite observar un resumen de las ID VLAN creadas, con sus puertos asignados, además permite habilitar los puertos que trabajaran en modo Trunk, y el tipo de encapsulamiento 802.1.Q

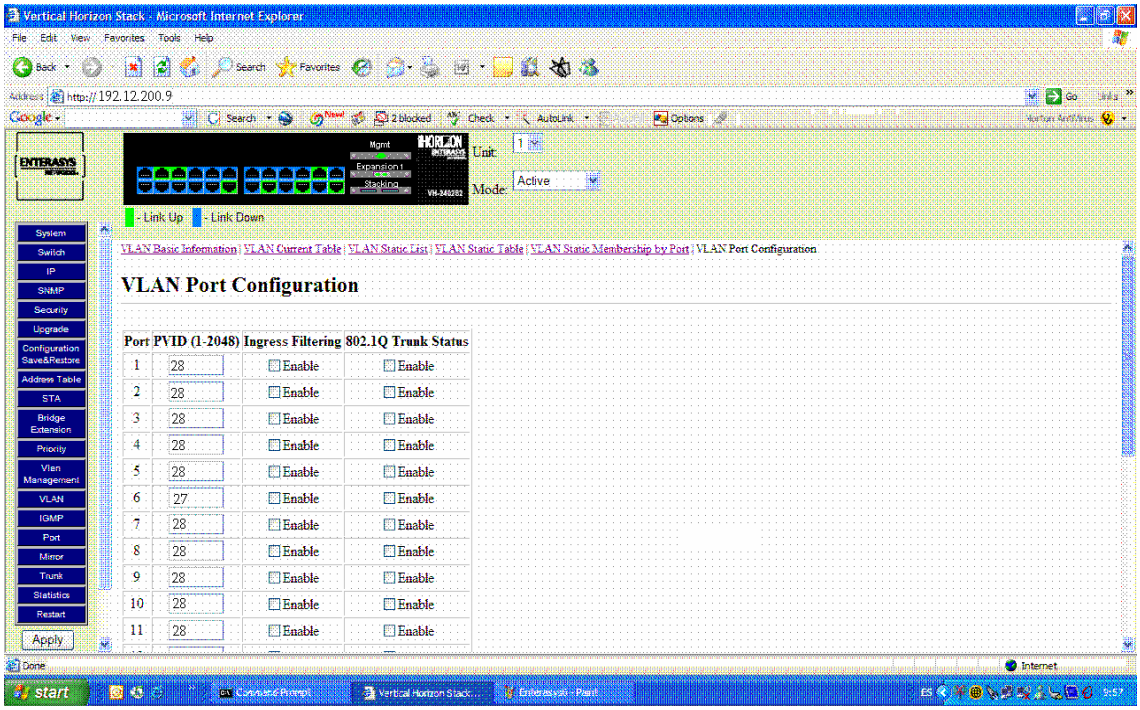


Figura 4.16: Habilitación del puerto Trunk y encapsulamiento 802.1.Q

4.4.4 Configuración de las Vlans en Router SSR 8600

En el Anexo G se puede observar la configuración de las VLANs creadas en el router SSR 8600

ANEXO G (CONFIGURACIONES DEL SSR 8600)

4.5 PRUEBAS DE CONECTIVIDAD ENTRE VLANS

Una vez configuradas las VLANs se debe realizar pruebas para ver el efecto de la configuración entre estas pruebas tenemos:

1. Pruebas de conectividad entre VLANs:

Para esta prueba se debe de disponer de por lo menos dos PCs que pertenezcan lógicamente a una misma VLAN, se debe realizar las siguientes pruebas.

1. Realizar un **ping** de la una PC a la otra, si se observa que entre ambas estaciones se responden esto indicara que están configurados en una misma VLAN.
2. Si de los dos PCs anteriores uno se coloca en un puerto de otra VLAN distinta y que no tengan permisos de comunicación entre estas dos. Se debe realizar un ping, se observara que no existe conectividad entre estas estaciones.

2. Pruebas de conectividad a nivel de aplicaciones.

Para la realización de estas pruebas los servidores de aplicaciones deben estar levantados y en plena producción. A continuación se debe realizar lo siguiente:

1. Con una PC ubicada en cualquier VLAN que se ha configurado se debe acceder a las aplicaciones que esta VLAN tiene el acceso permitido, con esta prueba verificaremos que la VLAN esta correctamente configurada y tiene el acceso a las aplicaciones.
2. Con una PC que pertenezca a una VLAN por ejemplo de LOGISTICA intentar acceder a otra VLAN por ejemplo de SERVIDORES para tratar de realizar cambios en los archivos de algún servidor, si no tiene los permisos no podrá visualizar las estaciones de la VLAN

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el Departamento de Comunicaciones se ha creado una VLAN de administración que tiene los privilegios de reconfigurar los equipos activos de red, habilitar o negar acceso a servicios como, Internet, correo electrónico, aplicaciones propietarias de la CGFT, con la finalidad de poder administrar eficientemente la red, habilitar servicios y permisos a los usuarios de las VLANs de acuerdo a los requerimientos que los solicite cada Departamento de la CGFT y poder resolver eficazmente algún problema de la red, para lo cual el personal de administración debe conocer o disponer del login y password para poder ingresar y realizar los cambios necesarios en los equipos activos (switch y routers), especialmente en el switch router SSR 8600, que es la parte medular o importa de la red (CORE).

- EL propósito de las recomendaciones de políticas de seguridad y administración expuestas en el presente trabajo es con la finalidad de generar en la CGFT una inquietud que incite a futuras investigaciones o proyectos que profundicen en el campo de la seguridad informática que es necesaria en toda empresa.

- La aplicación de VLANs, permite crear grupos de trabajo como si estos grupos pertenecieran a diferentes switches a pesar que estén conectados a un mismo switch permitiendo la utilización adecuada de todos los puertos de un Switch, mejorando la seguridad y administración entre los diferentes grupos de trabajo creados(VLANs).

- Los equipos activos de red de los que dispone la CGFT están diseñados para niveles corporativos, los cuales se los puede comparar con equipos encontrados en instituciones bancarias del país.

- Los equipos activos de la red de la CGFT, cumplen con la mayoría de estándares de la industria, permitiendo la administración y configuración de sus equipos para cumplir con las necesidades de la institución, estando dependiente del grado de conocimiento y experiencia del personal que administra la red.

- Por las características de rotación del personal militar del área de comunicaciones de la CGFT, es indispensable la elaboración de documentación que sirva como instructivo de procedimientos, para modificaciones, administración y control de la red, así como también se debe registrar un histórico de las soluciones dadas y de la evolución de la red.

- La falta de capacitación y soporte por parte del fabricante respecto al router SSR 8600 en combinación con la poca experiencia técnica con este equipo y la restricciones respecto a la manipulación de los equipos activos de la red por parte de la institución no han permitido aprovechar todas las bondades que estos equipos podrían brindar.

- Para una administración segura de los switches, se ha creado la VLAN llamada SWITCHES la misma que contiene todas las direcciones ips que corresponden a estos dispositivos, con la característica de que no se ha asignado puertos en los switches de piso.

- Debido al crecimiento desordenado de la red, la Dirección de Comunicaciones y Sistemas (DICOMSI) de la CGFT., consideró dentro de la Planificación Estratégica Institucional, proyectos integradores para modernizar los servicios de comunicaciones e informática ejemplo:

normalización del cableado estructurado a estándares Internacionales, creación de VLANs, optimización de los recursos que dispone la red informática, compra de un servidor DHCP.

- La tendencia de los administradores de red es la utilización de switches, porque permiten en una forma más fácil y cómoda la administración de la red, disminuye las colisiones en la red y aumenta un grado más de seguridad con la creación de VLANs

- Para controlar el tráfico entre las VLAN (enrutado) se utiliza las listas de control de acceso (ACL, Access Control List) las cuales nos permiten establecer los accesos entre las diferentes VLANs, estas listas se lo crea o se configura en el enrutador (Router).

- EL presente proyecto, ha permitido clarificar y consolidar los conocimientos respecto a las funcionalidades y capacidades entre los equipos activos de la red especialmente switches y routers, combinarlas con la finalidad de construir eficientes redes escalables.

5.2 RECOMENDACIONES

- Cuando se diseñe y se implemente una nueva red informática se debe diseñar en lo posible con equipos activos, (switch, router), de una misma marca de fabricación con la finalidad de poder explotar al máximo todos los beneficios que nos da cada fabricante, porque cuando se utiliza equipos de diferente fabricante algunas características técnicas de un fabricante no son compatibles con las de otro fabricante, pese a que los dos equipos estén estandarizados para realizar una función especifica, por ejemplo creación de VLans con el Estandar 802.1Q.

- Para el esquema de direcciones IP de una Intranet se debe utilizar o hacer referencia al estándar de direcciones privadas de la RFC 1597. Que nos

explica la correcta utilización de las direcciones IP. Y nos sugiere hacer uso de las recomendaciones de la IANA (autoridad de asignación de números de Internet).

- Es importante conocer los servicios y aplicaciones instalados en cada servidor y los requisitos que necesita cada Departamento o Grupo de Trabajo, con la finalidad de recopilar toda la información necesaria para poder plantear un diseño acorde a las necesidades de la institución.

- Los estandares que manejan los equipos Enterasys es soportada por los equipos Cisco, este aspecto es muy importante de tomar en cuenta para futuras ampliaciones de la red, ya que en un determinado momento se podría combinar ambos equipos (Enterays y Cisco) para diseñar la solución en base a VLANs.
- Al ser Cisco la empresa que lidera y define los estándares y tendencia en el mercado es recomendable reemplazar los equipos Enterasys por equipos Cisco, tanto en ampliaciones de la red como en reemplazo de equipos Enterasys dañados.

- Se recomienda unificar todos los equipos activos a Cisco, así se garantizaría que la red presente características de alto rendimiento, fiabilidad, simplicidad y escalabilidad, a todo esto se debe añadir el permanente soporte técnico por parte de Cisco, a costos razonables en el mercado, lo cual es una falencia con los equipos Enterasys, ya que no existe soporte en nuestro país.

- La aplicación de tecnología debe ofrecer como resultado una red que brinde un servicio eficaz, eficiente, seguro y accesos rápidos a recursos, de tal forma que los usuarios de la red sean los primeros en notar las mejoras, por lo cual se recomienda que el usuario reciba la debida capacitación para que conozca, acepte y utilice los recursos y servicios

tecnológicos que la institución le ofrece, bajo las normas y reglamentos que se deben establecer para su correcto uso.

- En el desarrollo de la investigación, implantación y configuración de las VLANs, es necesario planificar y seguir un procedimiento organizado y bien estructurado de tal forma que garantice el éxito del proyecto, cumpliendo tiempos de ejecución, predicción de imprevistos, distribución de los recursos, capacitación del personal.

- La recomendación y selección de un equipo activo de red, debe ser tomada en base al análisis de las funcionalidades que prestan (manual del fabricante), compatibilidades especialmente con Cisco, escalabilidad, soporte por el fabricante, stock de partes y repuestos.

- Al ser el core la parte fundamental del diseño de las Vlans y del funcionamiento de toda la red de la institución, se recomienda disponer de un equipo redundante (de preferencia Cisco) a manera de Contingencia, el cual reemplazara al equipo Enterasys 8600 en caso de daño

- Las funciones del Administrador de la red deben ser bien definidas especialmente en empresas con gran número de usuarios (bancos, ejercito, entidades de estado), en donde se tiene problemas de red, comunicación, aplicación, disponibilidad de recursos ,manejo de base de datos, deberían existir áreas que den el soporte adecuado a cada problema, así se recomienda personal para administrar la red, administrar la base de datos, administrar aplicaciones y sistemas operativos, complementando con la aplicación de políticas de administración y seguridad.

- Se recomienda que los puertos no utilizados en los switches de piso, se les asigne a una VLAN, por ejemplo llamada invitados, en la misma que se ha negado todos los servicios de la red, de esta forma se limita y controla posibles ingresos de personas no autorizadas.

- En el presente proyecto se uso direcciones IP tipo C (192.168.# VLAN.X) en donde el tercer byte identifica a la VLAN, esta asignación se la realizo por pedido del usuario, esta asignación no facilita la administración de la red ya que no indica mayores detalles de ubicación, o número de equipos, por lo cual se recomienda usar otros esquemas para la asignación de las direcciones IP, por ejemplo: una red tipo C con la siguiente distribución: 192.#PISO.#VLAN.X, donde el segundo byte indica el piso donde se encuentra un equipo activo que manejara la VLAN, el tercer byte indicara el numero de VLAN en ese piso, ejemplo. 192.10.5.254 en donde se interpretara que se hace referencia a la VLAN 5 que esta ubicada en el piso 10.

- Una red correctamente diseñada debe cumplir objetivos esenciales como son: escalabilidad para permitir un crecimiento de la organización, disponibilidad mediante la inclusión de redundancia, seguridad para la protección de datos y la infraestructura frente a ataques e intentos de robo y facilidad de administración en la configuración, la supervisión continua del estado y la detección de errores. Por tanto se recomienda que la arquitectura que disponga la CGFT tenga mecanismos redundantes de enrutamiento, de forma que en caso de error siempre haya componentes en funcionamiento que puedan atender las solicitudes. De igual manera para los sistemas de aplicaciones de los usuarios de la CGFT se debe tener alta disponibilidad y escalabilidad esto se puede lograr mediante el equilibrio de carga y la organización en clústeres con conmutación. Debido a que cuando se produce un error en el nodo principal que atiende las solicitudes, éstas se dirijan automáticamente a un nodo secundario. El nodo secundario debe tener acceso al mismo espacio de almacenamiento de datos que el nodo que ha fallado.

GLOSARIO DE TÉRMINOS

B

Backbone: La columna vertebral de la Red.

Backup: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

Bit (binary digit): Unidad básica de información representada por ceros y unos que se van sucediendo para conformar los distintos significados.

Browser: Navegador para poder visualizar las páginas Web en Internet.

Byte: Medida básica de capacidad en informática. Comprende 8 bits o interruptores, cada uno de los cuales puede conmutar en dos posiciones ON y OFF.

C

Caché: Carpeta o memoria intermedia que almacena temporalmente los archivos del equipo.

Correo electrónico: Mensajes, documentos, archivos que se envían personas a través de Internet o de una red.

Cortafuegos (firewall): Programa que protege a una red de otra red.

D

Dirección IP: Cadena numérica que identifica a una máquina en una red IP.

DNS: Sistema de Nombres por Dominio utilizado en Internet y basado en una estructura jerárquica y mediante el cual comunicamos con otro ordenador que puede encontrarse en otra parte del mundo.

Dominio: Grupo de equipos conectados en red que comparten información y recursos.

E

Extranet: Red basada en Internet de una compañía en la que comparte información y comunicación con agentes externos.

F

Firewall: Dispositivos de seguridad a entradas no autorizadas.

FTP (Protocolo de Transferencia de Ficheros): Transferir ficheros entre ordenadores en Internet.

G

Gateway (Puerta de acceso): Dispositivo que permite conectar entre sí dos redes normalmente de distinto protocolo o bien un servidor a una red.

Gigabyte (GB): Medida de 1.000 Mb (unos 1.000 millones de caracteres).

Grupos de trabajo: Conjunto de equipos conectados en red y que comparten los mismos recursos.

H

Host: Anfitrión, es cualquier ordenador que tiene un número IP y que puede tanto enviar como recibir información por una red.

HTTP: Protocolo de Transferencia de Hipertexto o entorno gráfico de las páginas Web.

I

Internet: Red de redes mundial. Telaraña o entramado mundial. También llamada World Wide Web (WWW), conjunto de redes que permiten la comunicación de millones de usuarios de todo el mundo.

Intranet: Red privada dentro de una organización que utiliza los protocolos propios de Internet.

IP: Dirección numérica y única de cada ordenador en Internet.

M

Módem (modulador/demodulador): Dispositivo que transmite datos desde un equipo a otro a través de la línea telefónica.

P

Password: Clave secreta personal.

Proveedor de Servicios Internet (ISP): Organización que proporciona acceso a Internet mediante una tarifa y que nos ofrece una serie de servicios.

Proxy: Servidor que realiza la conexión a Internet y que sirve de puerta de entrada a los ordenadores cliente.

S

Servidor: Equipo que controla el acceso de los usuarios a una red y les da servicio e información.

T

TCP/IP: Protocolo de Internet (Protocolo de Control de Transmisión/Protocolo Internet) que específica cómo se transmiten los datos en Internet para que todos los sistemas hablen el mismo idioma en Internet.

Telnet: Servicio que permite la conexión remota con cualquier ordenador de la red situado en cualquier parte del mundo como si de una terminal más se tratase.

W

WAN (Wide Area Network): Red pública de área extensa, no tiene límites físicos.

REFERENCIAS BIBLIOGRAFICAS

"**1**" **TANENBAUM**, Comer. Teorías de Comunicación de Datos y Redes de Datos, 2nd ed. Prentice Hall, 1989.

"**2**" Enterasys VH2402S 24 puertos X-Peditión User reference Manual

"3" Eduardo Collado Cabeza, Las VLAN, 11 de Enero de 2004 [pdf]

"4" http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link8 REDES LOCALES VIRTUALES Marzo del 2005

"5" http://lauca.usach.cl/~lsanchez/Vlan/#BENEFICIOS Virtual VLANs Marzo del 2005

"6" http://www.die.udec.cl/~redes/apuntes/myapuntes/node75.html#TB:WG802 Estandarización de Redes LAN Marzo del 2005

"7" Ing. José Joskowicz, REDES DE DATOS Instituto de Ingeniería Eléctrica, Facultad de Ingeniería Montevideo, Uruguay Agosto 2004 Versión 2

"8" **IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization** http://www.javvin.com/protocol8021P.html Abril del 2005

"9" **Spanning Tree Protocol in IEEE 802.1D** http://www.javvin.com/protocolSTP.html Marzo Del 2005

"10" Sánchez Paucar Edwin Patricio**,** METODOLOGIA PARA EL DISEÑO DE REDES VIRTUALES VLANS, 2000

"**11**" Best,J.W. Como investigar en educación, p. 7.

”[12]” Información proporcionada por los Administradores del Departamento de Comunicaciones

”[13]” http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link8 REDES LOCALES VIRTUALES

”[14]” http://lauca.usach.cl/~lsanchez/Vlan/#BENEFICIOS Virtual VLANs

BIBLIOGRAFIA

TANENBAUM, Comer. **Teorías de Comunicación de Datos y Redes de Datos**, 2nd ed. Prentice Hall, 1989.

Sánchez Paucar Edwin Patricio**, METODOLOGIA PARA EL DISEÑO DE REDES VIRTUALES VLANS**, 2000

Ing. José Joskowicz, **REDES DE DATOS** Instituto de Ingeniería Eléctrica, Facultad de Ingeniería Montevideo, Uruguay Agosto 2004 Versión 2

Eduardo Collado Cabeza, **Las VLAN**, 11 de Enero de 2004 [pdf]

María Dolores Cerini – Pablo Ignacio Prá **PLAN DE SEGURIDAD INFORMÁTICA,** Octubre 2002

Estandarización de Redes LAN
http://www.die.udec.cl/~redes/apuntes/myapuntes/node75.html#TB:WG802
Marzo del 2005

Guía de arquitectura de referencia de Internet Data Center
http://www.microsoft.com/spain/technet/guias/internet_datacenter.mspx Agosto del 2005

Seguridad en una Intranet
http://www.monografias.com/trabajos6/sein/sein.shtml Septiembre del 2005

XPEDITION**, User Reference Manual,** Marzo del 2004 [pdf]

IEEE 802.1q – VLAN http://standards.ieee.org/getieee802/802.1.html

IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
http://www.javvin.com/protocol8021P.html Abril del 2005

Spanning Tree Protocol in IEEE 802.1D http://www.javvin.com/protocolSTP.html Marzo del 2005

ANEXOS

ANEXO A

ENTREVISTAS

ENTREVISTAS:

La entrevista es la relación más directa entre el investigador y el objeto de estudio a través de individuos o grupos con el fin de obtener testimonios orales.

Para esto se debe realizar un cuestionario, el mismo que debe ser muy sencillo para ser comprendido con facilidad, y redactada en forma clara y precisa a fin de que se refiera directamente al punto de información deseado.

Para esto las preguntas o ítems pueden ser:

- Cerradas cuando se contestan con un si o un no.
- Abiertas cuando se contestan a criterio y juicio del entrevistado.
- En abanico cuando se presenta una serie de posibilidades para responder, entre las cuales el entrevistado escogerá la que crea conveniente.

Para la recopilación de información misma que será usada en el estudio y análisis del proyecto se utilizo las entrevistas, la razón fundamental de utilizar estas forma de recopilación de datos es por las restricciones que existen en el acceso a las diferentes Direcciones que conforman la CGFT y sobretodo que toda decisión y planteamientos de proyectos con la administración de la red es entre el Director de Comunicaciones y personal a cargo de su administración previa autorización del Comandante General del Ejercito.

Para esto se tuvo que establecer múltiples entrevistas así tenemos:

PRIMERA REUNION

Quito 27 de Octubre del 2004

REUNION CON EL DIRECTOR DE COMUNICACIONES DE LA FUERZA TERRESTRE

En esta primera reunión se trato en forma general de necesidades o problemas que se tenía en la CGFT manifestado por el Director de Comunicaciones.

En esta reunión se trataron:

- La posibilidad de brindar el servicio de Internet a todos los usuarios de la CGFT debido que hasta el momento solo determinado número de usuarios disponía de este servicio.
- Crear algún procedimiento o método para establecer seguridad de la información que maneja las diferentes Direcciones que conforma la CGFT.
- Para esto se planteo la creación de las redes Virtuales (VLANS) para mejorar la seguridad entre grupos de trabajo y la posibilidad de aumentar el servicio de Internet a los usuarios que no lo disponían. Previo a la realización de un análisis de la infraestructura tecnológica que disponían hasta el momento y de la topología de red que tenían configurado.

En esta reunión se acordó prestar todas las facilidades del caso para el estudio del proyecto con ciertas restricciones que serian impuestas a lo largo del proyecto por motivos de confidencialidad por ser una institución que brinda seguridad nacional al país.

Finalmente nos pusieron a cargo de la persona que administraba la red informática el Sr. Capitán Hugo Álvarez el cual nos facilitaría toda la información necesaria para la realización del proyecto.

SEGUNDA REUNION

Quito 16 de Noviembre del 2004

REUNION CON EL SR. CAPITAN HUGO ALVAREZ ENCARGADO DE LA ADMINISTRACION DE LA RED INFORMATICA

En esta reunión se trataron puntos de interés que se debían tomar en cuenta para la realización del proyecto:

Puntos tratados:

- La necesidad de realizar un estudio y análisis de la red informática para conocer su situación actual y establecer una solución que satisfaga los requerimientos planteados por el Director de Comunicaciones.
- Establecer un mecanismo para la obtención de información que se necesita para el estudio y análisis del proyecto. Para esto se planteo, realizar encuestas, con la utilización de cuestionarios y formulario que debían ser llenados por los usuarios que hacen uso de la red y personal que administra la misma.

Ante estos puntos planteados el Capitán Hugo Álvarez nos manifestó que lo planteado hasta el momento debería ser estudiado y discutido con el Director de Comunicaciones el cual es la máxima autoridad y daría la aprobación o plantaría otra forma, de que los datos nos sean facilitados para la continuación del proyecto, previa una reunión que ellos tendrían.

TERCERA REUNION

Quito 5 de Enero del 2005

REUNION CON EL SR. CAPITAN HUGO ALVAREZ ENCARGADO DE LA ADMINISTRACION DE LA RED INFORMATICA

En esta reunión se trataron puntos de interés para las dos partes:

Puntos tratados:

- Establecer los formatos para la recopilación de datos.
- Modificación de Direcciones IP reales por Direcciones IP ficticias para conservar la confidencialidad de la información que maneja la CGFT.
- Los usuarios con sus respectivas contraseñas deberán ser cambiados como también sus grupos de trabajo y respectivos departamentos.
- Toda la información que se recopilará, deberá ser revisara previamente y se publicaría solo lo necesario o lo que autorice la CGFT.

El Sr. Capitán Hugo Álvarez se compromete a facilitar toda la información que crea necesaria, para continuar con el proyecto, para esto se estableció un periodo de tiempo de tres meses, para la recopilación y selección de la información.

CUARTA REUNION

Quito 4 de Mayo del 2005

REUNION CON EL CAPITAN HUGO ALVAREZ ENCARGADO DE LA ADMINISTRACION DE LA RED INFORMATICA

Puntos tratados:

- Recomendaciones y restricciones, en cuanto al manejo de la información proporcionada
- Entrega de información de parte de la CGFT tanto de usuarios como de equipos activos y red informática.
- Se realizo una evaluación preliminar de la red, con información que hasta el momento se había recopilado, complementándola con información verbal que el administrador de la red expuso, y se llego a las primeras conclusiones:

    1. Existe una sub utilización de los equipos activos de la CGFT por tener las dos redes Internet e Intranet separados.
    2. La necesidad de unificación de las dos redes Internet e Intranet para poder mejorar los servicios a todos los usuarios que lo necesiten porque en la actualidad por ejemplo el servicio de Internet es limitado.
    3. El mejoramiento de la seguridad de la información que circula por la red informática debido al crecimiento desordenado de las redes de datos en el Edificio de la CGFT.
    4. Actualmente la CGFT no dispone de un diseño y topología de red definida.

- Por las características de los equipos activos de red que dispone la CGFT se propuso la creación de VLANs que cubriría los problemas y necesidades de la institución, plantendose:

    1. La creación de VLANs de acuerdo a los grupos de trabajo que existían en la CGFT
    2. La configuración de permisos de acceso entre VLANs creadas de acuerdo al requerimiento que se establezca entre administrador y usuarios para mejorar la seguridad de la información que fluye a través de la red.
    3. La unificación de las dos redes Internet e Intranet para poner a disposición todos los servicios, de acuerdo a los requerimientos de cada dirección.
    4. La reutilización y reubicación de los equipos activos de red, que cumplan con las especificaciones técnicas y estándares para la creación de redes VLANs.

Finalmente con toda la información entregada se decidió seguir con la siguiente etapa que es el análisis de toda la información y la presentación de una propuesta que satisfaga los requerimientos establecidos.

ANEXO B
FORMATO DE ENTREVISTAS

USUARIOS

NOMBRE DE USUARIO	FUNCION QUE DESEMPEÑA	SERVICIOS Y APLICACIONES QUE UTILIZA				

ANEXO B1: Formato para el Inventario de Usuarios

SERVIDORES

NOMBRE	FUNCIONALIDAD	FIJA/MOVIL	INTERFAZ ETHERNET		PROTOCOLOS		DIRECCION	SERVICIOS Y APLICACIONES
			10 MHZ	10/100 MHZ	NETBEUI	TCP/IP	TCP/IP TIPO	
PISO 0								
PISO 1								

ANEXO B2: Formato para el Inventario de Servidores

ESTACIONES

NOMBRE	FIJA/MOVIL	USUARIOS	INTERFAZ ETHERNET		PROTOCOLOS		DIRECCION	SERVICIOS Y APLICACIONES				
			10 MHZ	10/100 MHZ	NETBEUI	TCP/IP	TCP/IP TIPO					
PISO 0												
PISO 1												

ANEXO B3: Formato para el Inventario de Estaciones

INVENTARIO DE EQUIPOS ACTIVOS

HUBS	
NOMBRE	
PISO	
MARCA	
PUERTOS LIBRES	
OCUPADOS	
UPLINK	

SWITCHS	
NOMBRE	
PISO	
MARCA	
PUERTOS LIBRES	
OCUPADOS	

ROUTERS	
NOMBRE	
PISO	
MARCA	
PUERTOS LIBRES	
OCUPADOS	

NEXO B4: Formato para el Inventario de Equipos Activos

ANEXO C

INVENTARIO USUARIOS CGFT

USUARIOS QUE CONFORMAN LA RED DE LA CGFT

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
	10								
		centromen	1				192.168.10.1		
				1	centro001	centro001	192.168.10.10	1	Recepción centro de mensajes
				2	centro002	centro002	192.168.10.11	2	Jefe centro de Mensajes
		doctrina	2				192.168.10.2		
				1	doctrina001	doctrina001	192.168.10.12	3	Administrativo de Doctrina
				2	doctrina002	doctrina002	192.168.10.13	4	Ayudante de Doctrina
ENTERASYS									
SWITCH VH2402S (2)	9								
		planificacion	3				192.168.9.1		
				1	planificacion001	planificacion001	192.168.9.11	5	Administrativo planificación
				2	planificacion002	planificacion002	192.168.9.12	6	Secretaria planificación
		planificacion1	4				192.168.9.2		
				1	planificacion1001	planificacion1001	192.168.9.12	7	Jefe planificación
				2	planificacion1002	planificacion1002	192.168.9.13	8	Subjefe planificacion
				3	planificacion1003	planificacion1003	192.168.9.14	9	Asesor planificacion
				4	planificacion1004	planificacion1004	192.168.9.15	10	Educación de planificacion
				5	planificacion1005	planificacion1005	192.168.9.16	11	Doctrina de planificacion
				6	planificacion1006	planificacion1006	192.168.9.17	12	Planificación de planificacion
				7	planificacion1007	planificacion1007	192.168.9.18	13	Inteligencia de planificacion
				8	planificacion1008	planificacion1008	192.168.9.19	14	Operaciones de planificacion
				9	planificacion1009	planificacion1009	192.168.9.20	15	comunicaciones de planificacion
				10	planificacion1010	planificacion1010	192.168.9.21	16	Organización de planificacion
				11	planificacion1011	planificacion1011	192.168.9.22	17	Inspectoria de planificacion
				12	planificacion1012	planificacion1012	192.168.9.23	18	Personal de planificacion
				13	planificacion1013	planificacion1013	192.168.9.24	19	Bienestar de personal de planificacion
				14	planificacion1014	planificacion1014	192.168.9.25	20	Sanidad de planificacion
				15	planificacion1015	planificacion1015	192.168.9.26	21	Comunicación social de planificacion
				16	planificacion1016	planificacion1016	192.168.9.27	22	Logística de planificacion
				17	planificacion1017	planificacion1017	192.168.9.28	23	Finanzas de planificacion
				18	planificacion1018	planificacion1018	192.168.9.29	24	Mantenimiento de planificacion

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
	9	organización	5				192.168..9.3		
				1	organizacion001	organizacion001	192.168.9.40	1	Servidor de organización
				2	organizacion002	organizacion002	192.168.9.41	2	Organización de cien
				3	organizacion003	organizacion003	192.168.9.42	3	Orgánico Shyris
				4	organizacion004	organizacion004	192.168.9.43	4	Orgánico Tarqui
				5	organizacion005	organizacion005	192.168.9.44	5	Orgánico Logística
				6	organizacion006	organizacion006	192.168.9.45	6	Orgánico Amazonas
				7	organizacion007	organizacion007	192.168.9.46	7	Orgánico Libertad
				8	organizacion008	organizacion008	192.168.9.47	8	Orgánico comandancia general
				9	organizacion009	organizacion009	192.168.9.48	9	Jefe oficina Organización
				10	organizacion010	organizacion010	192.168.9.49	10	Supervisión Organización
				11	organizacion011	organizacion011	192.168.9.50	11	user1
				12	organizacion012	organizacion012	192.168.9.51	12	user2
		espe	6				192.168.9.4		
				1	espe0001	espe0001	192.168.9.200	13	Usuario espe001
				2	espe0002	espe0002	192.168.9.201	14	Usuario espe002
				3	espe0003	espe0003	192.168.9.202	15	Usuario espe003
				4	espe0004	espe0004	192.168.9.203	16	Usuario espe004
				5	espe0005	espe0005	192.168.9.204	17	Usuario espe005
				6	espe0006	espe0006	192.168.9.205	18	Usuario espe006
				7	espe0007	espe0007	192.168.9.206	19	Usuario espe007
				8	espe0008	espe0008	192.168.9.207	20	Usuario espe008
				9	espe0009	espe0009	192.168.9.208	21	Usuario espe009
				10	espe0010	espe0010	192.168.9.209	22	Usuario espe010
				11	espe0011	espe0011	192.168.9.210	23	Usuario espe011
				12	espe0012	espe0012	192.168.9.211	24	Usuario espe012
				13	espe0013	espe0013	192.168.9.212		Usuario espe013
	8								
		comunicaciones	7				192.168.8.1		
				1	comunicaciones001	comunicaciones001	192.168.8.10	1	Director comunicaciones
				2	comunicaciones002	comunicaciones002	192.168.8.11	2	Subdirector comunicaciones
				3	comunicaciones003	comunicaciones003	192.168.8.12	3	Secretaria comunicaciones
				4	comunicaciones004	comunicaciones004	192.168.8.13	4	usuario comunicaciones
				5	comunicaciones005	comunicaciones005	192.168.8.14	5	usuario comunicaciones

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
	8			6	comunicaciones006	comunicaciones006	192.168.8.15	6	usuario comunicaciones
				7	comunicaciones007	comunicaciones007	192.168.8.16	7	usuario comunicaciones
				8	comunicaciones008	comunicaciones008	192.168.8.17	8	usuario comunicaciones
				9	comunicaciones009	comunicaciones009	192.168.8.18	9	usuario comunicaciones
				10	comunicaciones010	comunicaciones010	192.168.8.19	10	usuario comunicaciones
				11	comunicaciones011	comunicaciones011	192.168.8.20	11	usuario comunicaciones
				12	comunicaciones012	comunicaciones012	192.168.8.21	12	usuario comunicaciones
				13	comunicaciones013	comunicaciones013	192.168.8.22	13	usuario comunicaciones
				14	comunicaciones014	comunicaciones014	192.168.8.23	14	usuario comunicaciones
				15	comunicaciones015	comunicaciones015	192.168.8.24	15	usuario comunicaciones
				16	comunicaciones016	comunicaciones016	192.168.8.25	16	usuario comunicaciones
				17	comunicaciones017	comunicaciones017	192.168.8.26	17	usuario comunicaciones
		inspectoria	8				192.168.8.2		
				1	inspectoria001	inspectoria001	192.168.8.27	18	Administrativo de inspectoria
				2	inspectoria002	inspectoria002	192.168.8.28	19	Ayudante de inspectoria
				3	inspectoria003	inspectoria003	192.168.8.29	20	Contraloria de inspectoria
ENTERASYS				4	inspectoria004	inspectoria004	192.168.8.30	21	Auditoria de inspectoria
SWITCH VH2402S (1)	7								
		inteligencia	9				192.168.7.1		
				1	inteligencia001	inteligencia001	192.168.7.10	22	Administrativo de inteligencia
				2	inteligencia002	inteligencia002	192.168.7.11	23	Ayudante de inteligencia
	6								
		comunicasocial	10				192.168.6.1		
				1	comunicasocial001	comunicasocial001	192.168.6.10	1	Administrativo comunicación social
				2	comunicasocial002	comunicasocial002	192.168.6.11	2	Ayudante de comunicación social
		educacion	11				192.168.6.2		
				1	educacion001	educacion001	192.168.6 .12	2	Administrativo de educación
ENTERASYS				2	educacion002	educacion002	192.168.6.13	4	Ayudante de educación
SWITCH VH2402S (1)	5								
		operaciones	12				192.168.5.1		
				1	operaciones001	operaciones001	192.168.5.10	5	Administrativo de operaciones

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
				2	operaciones002	operaciones002	192.168.5.11	6	Ayudante de operaciones
				3	operaciones003	operaciones003	192.168.5.12	7	Instrucción Administrativo
				4	operaciones004	operaciones004	192.168.5.13	8	Educación física administrativo
		comandocontrol	13				192.168.5.2		
				1	comandocontrol001	comandocontrol001	192.168.5.14	9	Administrativo comando control
				2	comandocontrol002	comandocontrol002	192.168.5.15	10	Ayudante comando control
	4								
		ciemgeneral	14				192.168.4.1		
				1	ciemgeneral001	ciemgeneral001	192.168.4.10	1	Administrativo de ciem
				2	ciemgeneral002	ciemgeneral002	192.168.5.11	2	Ayudante de ciem
				3	ciemgeneral003	ciemgeneral003	192.168.4.12	3	Secretaria de ciem
		jefatura	15				192.168.4.2		
				1	jefatura001	jefatura001	192.168.4.13	4	Administrativo de jefatura
				2	jefatura002	jefatura002	192.168.4.14	5	Ayudante de jefatura
				3	jefatura003	jefatura003	192.168.4.15	6	Secretaria de jefatura
ENTERASYS				4	jefatura004	jefatura004	192.168.4.16	7	Asesor de jefatura
SWITCH VH2402S (1)	3								
		logistica	16				192.168.3.1		
				1	logistica001	logistica001	192.168.3.10	8	Administrativo de Logistica
				2	logistica002	logistica002	192.168.3.11	9	Ayudante de Logistica
		logistica1	17	1	logistica1001	logistica1001	192.168.3.12	10	Servidor de Logística Sun. S.S.20
				2	logistica1002	logistica1002	192.168.3.13	11	Servidor de Logística Sun. S.S.20
				3	logistica1003	logistica1003	192.168.3.14	12	Jefatura de Logística
				4	logistica1004	logistica1004	192.168.3.15	13	Subjefatura de Logística
				5	logistica1005	logistica1005	192.168.3.16	14	Administrativo de Logística1
				6	logistica1006	logistica1006	192.168.3.17	15	Planificación Logística
				7	logistica1007	logistica1007	192.168.3.18	16	Transporte Logística
				8	logistica1008	logistica1008	192.168.3.19	17	Presupuesto Logística
				9	logistica1009	logistica1009	192.168.3.20	18	centro Datos Logística
				10	logistica1010	logistica1010	192.168.3.21	19	centro Datos Logística
				11	logistica1011	logistica1011	192.168.3.22	20	centro Datos Logística
				12	logistica1012	logistica1012	192.168.3.23	21	Aereo Logística
				13	logistica1013	logistica1013	192.168.3.24	22	Ingenieria Logística

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
				14	logistica1014	logistica1014	192.168.3.25	23	Abas.mat. Guerra Logística
				15	logistica1015	logistica1015	192.168.3.26	1	Jefatura. Matt. Logística
				16	logistica1016	logistica1016	192.168.3.27	2	Abas. Trop. Logística
				17	logistica1017	logistica1017	192.168.3.28	3	Abastecimiento. Int. Logística
				18	logistica1018	logistica1018	192.168.3.29	4	Abastecimiento. Int. Logística
				19	logistica1019	logistica1019	192.168.3.30	5	Presupuest. Int. Logística
	2								
		logistica2	18				192.168.2.150		
				1	logistica2001	logistica2001	192.168.2.160	1	Administrativo de logística2
				2	logistica2002	logistica2002	192.168.2.161	2	Ayudante de logística2
		cuartelgeneral	19				192.168.2.151		
				1	cuartelgeneral001	cuartelgeneral001	192.168.2.162	3	Administrativo Cuartel G.
				2	cuartelgeneral002	cuartelgeneral002	192.168.2.163	4	Ayudante Cuartel G.
		sanidad	20				192.168.2.152		
				1	sanidad001	sanidad001	192.168.2.164	5	Administrativo de sanidad
				2	sanidad002	sanidad002	192.168.2.165	6	Ayudante de sanidad
		sanidad1	21				192.168.2.152		
				1	sanidad1001	sanidad1001	192.168.2.164	7	Administrativo de sanidad1
				2	sanidad1002	sanidad1002	192.168.2.165	8	Ayudante de sanidad1
ENTERASYS	1								
SWITCH VH2402S (3)		recursoshumanos	22				192.168.1.150		
				1	recursoshumanos001	recursoshumanos001	192.168.1.160	9	Reclutamiento oficiales
				2	recursoshumanos002	recursoshumanos002	192.168.1.161	10	Reclutamiento voluntarios
				3	recursoshumanos003	recursoshumanos003	192.168.1.162	11	Reclutamiento emcis.
				4	recursoshumanos004	recursoshumanos004	192.168.1.163	12	Capacitación militares y emcis
				5	recursoshumanos005	recursoshumanos005	192.168.1.164	13	Plan carrera
				6	recursoshumanos006	recursoshumanos006	192.168.1.165	14	Rectificaciones
				7	recursoshumanos007	recursoshumanos007	192.168.1.166	15	Pases oficiales
				8	recursoshumanos008	recursoshumanos008	192.168.1.167	16	Pases voluntarios
				9	recursoshumanos009	recursoshumanos009	192.168.1.168	17	Traslados emcis
				10	recursoshumanos010	recursoshumanos010	192.168.1.169	18	Becas y ayudantes administrativos
				11	recursoshumanos011	recursoshumanos011	192.168.1.170	19	Bajas cancelacion emcis
				12	recursoshumanos012	recursoshumanos012	192.168.1.171	20	Disponibilidades o/ a disposición
				13	recursoshumanos013	recursoshumanos013	192.168.1.172	21	Reservas

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
				14	recursoshumanos014	recursoshumanos014	192.168.1.173	22	Descuentos sueldos
				15	recursoshumanos015	recursoshumanos015	192.168.1.174	23	Pases, sueldos, comandados
				16	recursoshumanos016	recursoshumanos016	192.168.1.175	24	Descuento issfa, iess
				17	recursoshumanos017	recursoshumanos017	192.168.1.176	1	Condecoraciones
				18	recursoshumanos018	recursoshumanos018	192.168.1.177	2	Licencias y permisos
				19	recursoshumanos019	recursoshumanos019	192.168.1.178	3	Ascensos voluntarios
				20	recursoshumanos020	recursoshumanos020	192.168.1.179	4	Parte diario
				21	recursoshumanos021	recursoshumanos021	192.168.1.180	5	Usuario del Siper
				22	recursoshumanos022	recursoshumanos022	192.168.1.181	6	Usuario del Siper
				23	recursoshumanos023	recursoshumanos023	192.168.1.182	7	Usuario del Siper
				24	recursoshumanos024	recursoshumanos024	192.168.1.183	8	Usuario del Siper
				25	recursoshumanos025	recursoshumanos025	192.168.1.184	9	Usuario del Siper
				26	recursoshumanos026	recursoshumanos026	192.168.1.185	10	Usuario del Siper
				27	recursoshumanos027	recursoshumanos027	192.168.1.186	11	Usuario del Siper
				28	recursoshumanos028	recursoshumanos028	192.168.1.187	12	Usuario del Siper
				29	recursoshumanos029	recursoshumanos029	192.168.1.188	13	Usuario del Siper
				30	recursoshumanos030	recursoshumanos030	192.168.1.189	14	Usuario del Siper
				31	recursoshumanos031	recursoshumanos031	192.168.1.190	15	Usuario del Siper
				32	recursoshumanos032	recursoshumanos032	192.168.1.191	16	Usuario del Siper
				33	recursoshumanos033	recursoshumanos033	192.168.1.192	17	Usuario del Siper
				34	recursoshumanos034	recursoshumanos034	192.168.1.193	18	Usuario del Siper
				35	recursoshumanos035	recursoshumanos035	192.168.1.194	19	Usuario del Siper
				36	recursoshumanos036	recursoshumanos036	192.168.1.195	20	Usuario del Siper
				37	recursoshumanos037	recursoshumanos037	192.168.1.196	21	Usuario del Siper
				38	recursoshumanos038	recursoshumanos038	192.168.1.197	22	Usuario del Siper
				39	recursoshumanos039	recursoshumanos039	192.168.1.198	23	Usuario del Siper
				40	recursoshumanos040	recursoshumanos040	192.168.1.199	24	Usuario del Siper
				41	recursoshumanos041	recursoshumanos041	192.168.1.200	1	Usuario del Siper
				42	recursoshumanos042	recursoshumanos042	192.168.1.201	2	Usuario del Siper
				43	recursoshumanos043	recursoshumanos043	192.168.1.202	3	Usuario del Siper
				44	recursoshumanos044	recursoshumanos044	192.168.1.203	4	Usuario del Siper
				45	recursoshumanos045	recursoshumanos045	192.168.1.204	5	Usuario del Siper
				46	recursoshumanos046	recursoshumanos046	192.168.1.205	6	Usuario del Siper
				47	recursoshumanos047	recursoshumanos047	192.168.1.206	7	Usuario del Siper

EQUIPO UTILIZADO	UBICACION	GRUPO	ID GRUPO	# DE	USERNAME	USER NAME LOGIN	IP	PUERTO	DESCRIPCION USUARIOS
	PISO	DE TRABAJO		USUARIOS				SWITCH	
				48	recursoshumanos048	recursoshumanos048	192.168.1.207	8	Usuario del Siper
				49	recursoshumanos049	recursoshumanos049	192.168.1.208	9	Usuario del Siper
				50	recursoshumanos050	recursoshumanos050	192.168.1.209	10	Usuario del Siper
				51	recursoshumanos051	recursoshumanos051	192.168.1.210	11	Usuario del Siper
				52	recursoshumanos052	recursoshumanos052	192.168.1.211	12	Usuario del Siper
				53	recursoshumanos053	recursoshumanos053	192.168.1.212	13	Usuario del Siper
				54	recursoshumanos054	recursoshumanos054	192.168.1.213	14	Usuario del Siper
				55	recursoshumanos055	recursoshumanos055	192.168.1.214	15	Usuario del Siper
	PB								
		bienestarpersonal	23				192.168.11.1		
				1	bienestarpersonal001	bienestarpersonal001	192.168.11.10	1	Administrativo bienestar personal
				2	bienestarpersonal002	bienestarpersonal002	192.168.11.11	2	Ayudante bienestar personal
				3	bienestarpersonal003	bienestarpersonal003	192.168.11.12	3	Director bienestar personal
				4	bienestarpersonal004	bienestarpersonal004	192.168.11.13	4	Subsidio Familiar bienestar personal
				5	bienestarpersonal005	bienestarpersonal005	192.168.11.14	5	Vivienda Fiscal bienestar personal
Smart Switch ROUTER	subs								
8600(1)		bienestarpersonal1	24				192.168.12.1		
				1	bienestarpersonal1001	bienestarpersonal1001	192.168.12.10	6	Retenciones Judiciales bienestar personal1
				2	bienestarpersonal1002	bienestarpersonal1002	192.168.12.11	7	Subdirector bienestar personal1
		servidores	25				192.168.12.2		
				1	servidores001	servidores001	192.168.12.12	8	Servidor
				2	servidores002	servidores002	192.168.12.13	9	Servidor
				3	servidores003	servidores003	192.168.12.14	10	Servidor
				4	servidores004	servidores004	192.168.12.15	11	Servidor
		control	26				192.168.12.3		
				1	control001	control001	192.168.12.15	12	Administración Redes
				2	control002	control002	192.168.12.16	13	Administración Servidores

NEXO C1: Inventario de Usuarios de la CGFT

ANEXO D

DESCRIPCION DETALLADA DE VLAN CGFT

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
101				192.168.101.254		
	1	centro001	centro001	192.168.101.X	1	Recepción centro de mensajes
	2	centro002	centro002	192.168.101.X	2	Jefe Centro de Mensajes
102				192.168.102.254		
	1	doctrina001	doctrina001	192.168.102.X	3	Administrativo de Doctrina
	2	doctrina002	doctrina002	192.168.102.X	4	Ayudantia de Doctrina
103				192.168.103.254		
	1	planificacion001	planificacion001	192.168.103.X	5	Administrativo EMP
	2	planificacion002	planificacion002	192.168.103.X	6	Secretaria EMP
104				192.168.104.254		
	1	planificacion1001	planificacion1001	192.168.104.X	7	Jefe empft
	2	planificacion1002	planificacion1002	192.168.104.X	8	Subjefe
	3	planificacion1003	planificacion1003	192.168.104.X	9	Accesoria
	4	planificacion1004	planificacion1004	192.168.104.X	10	Educación
	5	planificacion1005	planificacion1005	192.168.104.X	11	Doctrina
	6	planificacion1006	planificacion1006	192.168.104.X	12	Planificicación
	7	planificacion1007	planificacion1007	192.168.104.X	13	Inteligencia
	8	planificacion1008	planificacion1008	192.168.104.X	14	Operaciones
	9	planificacion1009	planificacion1009	192.168.104.X	15	Dicomsi
	10	planificacion1010	planificacion1010	192.168.104.X	16	Organización
	11	planificacion1011	planificacion1011	192.168.104.X	17	Inspectoria
	12	planificacion1012	planificacion1012	192.168.104.X	18	Personal
	13	planificacion1013	planificacion1013	192.168.104.X	19	Bienestar de personal
	14	planificacion1014	planificacion1014	192.168.104.X	20	Sanidad
	15	planificacion1015	planificacion1015	192.168.104.X	21	Comunicación social
	16	planificacion1016	planificacion1016	192.168.104.X	22	Logística
	17	planificacion1017	planificacion1017	192.168.104.X	23	Finanzas
	18	planificacion1018	planificacion1018	192.168.104.X	24	Mantenimiento

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
105				192.168.105.254		
	1	organizacion001	organizacion001	192.168.105.X	1	Servidor de organización
	2	organizacion002	organizacion002	192.168.105.X	2	Organización de cien
	3	organizacion003	organizacion003	192.168.105.X	3	Orgánico Shyris
	4	organizacion004	organizacion004	192.168.105.X	4	Orgánico Tarqui
	5	organizacion005	organizacion005	192.168.105.X	5	Orgánico Logística
	6	organizacion006	organizacion006	192.168.105.X	6	Orgánico Amazonas
	7	organizacion007	organizacion007	192.168.105.X	7	Orgánico Libertad
	8	organizacion008	organizacion008	192.168.105.X	8	Orgánico cgft
	9	organizacion009	organizacion009	192.168.105.X	9	Jefe oficina Organización
	10	organizacion010	organizacion010	192.168.105.X	10	Supervisión Organización
	11	organizacion011	organizacion011	192.168.105.X	11	Subs. Rosero
	12	organizacion012	organizacion012	192.168.105.X	12	Emci. Jamil
106				192.168.106.254		
	1	espe0001	espe0001	192.168.106.X	13	Usuario Siper1 ESPE
	2	espe0002	espe0002	192.168.106.X	14	Usuario Siper2 ESPE
	3	espe0003	espe0003	192.168.106.X	15	Usuario Siper3 ESPE
	4	espe0004	espe0004	192.168.106.X	16	Usuario Siper4 EsPE
	5	espe0005	espe0005	192.168.106.X	17	Usuario Siper3 ESPE
	6	espe0006	espe0006	192.168.106.X	18	Usuario Siper4 EsPE
	7	espe0007	espe0007	192.168.106.X	19	Usuario Siper3 ESPE
	8	espe0008	espe0008	192.168.106.X	20	Usuario Siper4 EsPE
	9	espe0009	espe0009	192.168.106.X	21	Usuario Siper3 ESPE
	10	espe0010	espe0010	192.168.106.X	22	Usuario Siper4 EsPE
	11	espe0011	espe0011	192.168.106.X	23	Usuario Siper3 ESPE
	12	espe0012	espe0012	192.168.106.X	24	Usuario Siper4 EsPE
107				192.168.107.254		
	1	comunicaciones001	comunicaciones001	192.168.107.X	1	Director dicomsi
	2	comunicaciones002	comunicaciones002	192.168.107.X	2	Subdirector dicomsi
	3	comunicaciones003	comunicaciones003	192.168.107.X	3	Secretaria dicomsi
	4	comunicaciones004	comunicaciones004	192.168.107.X	4	

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
	5	comunicaciones005	comunicaciones005	192.168.107.X	5	Usuarios de comunicaciones
	6	comunicaciones006	comunicaciones006	192.168.107.X	6	Usuarios de comunicaciones
	7	comunicaciones007	comunicaciones007	192.168.107.X	7	Usuarios de comunicaciones
	8	comunicaciones008	comunicaciones008	192.168.107.X	8	Usuarios de comunicaciones
	9	comunicaciones009	comunicaciones009	192.168.107.X	9	Usuarios de comunicaciones
	10	comunicaciones010	comunicaciones010	192.168.107.X	10	Usuarios de comunicaciones
	11	comunicaciones011	comunicaciones011	192.168.107.X	11	Usuarios de comunicaciones
	12	comunicaciones012	comunicaciones012	192.168.107.X	12	Usuarios de comunicaciones
	13	comunicaciones013	comunicaciones013	192.168.107.X	13	Usuarios de comunicaciones
	14	comunicaciones014	comunicaciones014	192.168.107.X	14	Usuarios de comunicaciones
	15	comunicaciones015	comunicaciones015	192.168.107.X	15	Usuarios de comunicaciones
	16	comunicaciones016	comunicaciones016	192.168.107.X	16	Usuarios de comunicaciones
	17	comunicaciones017	comunicaciones017	192.168.107.X	17	Usuarios de comunicaciones
108				192.168.108.254		
	1	inspectoria001	inspectoria001	192.168.108.X	18	Administrativo de IGFT
	2	inspectoria002	inspectoria002	192.168.108.X	19	Ayudantia de IGFT
	3	inspectoria003	inspectoria003	192.168.108.X	20	Contraloria de IGFT
	4	inspectoria004	inspectoria004	192.168.108.X	21	Auditoria de IGFT
109				192.168.109.254		
	1	inteligencia001	inteligencia001	192.168.109.X	22	Administrativo de DIFT
	2	inteligencia002	inteligencia002	192.168.109.X	23	Ayudantia de DIFT
110				192.168.110.254		
	1	comunicasocial001	comunicasocial001	192.168.110..X	1	Administrativo JCS
	2	comunicasocial002	comunicasocial002	192.168.110.X	2	Ayudantia de JCS
111				192.168.111.254		
	1	educacion001	educacion001	192.168.111.X	3	Administrativo de DEFT
	2	educacion002	educacion002	192.168.111.X	4	Ayudantia de DEFT

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
112				192.168.112.254		
	1	operaciones001	operaciones001	192.168.112.X	5	Administrativo de operaciones
	2	operaciones002	operaciones002	192.168.112.X	6	Ayudantia de operaciones
	3	operaciones003	operaciones003	192.168.112.X	7	Instrucción Administrativo
	4	operaciones004	operaciones004	192.168.112.X	8	Educación física administrativo
113				192.168.113.254		
	1	comandocontrol001	comandocontrol001	192.168.113.X	9	Administrativo C3I2
	2	comandocontrol002	comandocontrol002	192.168.113.X	10	Ayudantia C3I2
114				192.168.114.254		
	1	ciemgeneral001	ciemgeneral001	192.168.114.X	1	Administrativo de CE
	2	ciemgeneral002	ciemgeneral002	192.168.114.X	2	Ayudantia de CE
	3	ciemgeneral003	ciemgeneral003	192.168.114.X	3	Secretariog de CE
115				192.168.115.254		
	1	jefatura001	jefatura001	192.168.115.X	4	Administrativo de JEM
	2	jefatura002	jefatura002	192.168.115.X	5	Ayudantia de JEM
	3	jefatura003	jefatura003	192.168.115.X	6	Secretariataria de JEM
	4	jefatura004	jefatura004	192.168.115.X	7	Asesoria de JEM
116				192.168.116.254		
	1	logistica001	logistica001	192.168.116.X	8	Administrativo de Logistica
	2	logistica002	logistica002	192.168.116.X	9	Ayudantia de Logistica
117	1			192.168.117.254	10	Servidor de Logística Sun. S.S.20
	2	logistica1001	logistica1001	192.168.117.X	11	Servidor de Logística Sun. S.S.20
	3	logistica1002	logistica1002	192.168.117.X	12	Jefatura de Logística
	4	logistica1003	logistica1003	192.168.117.X	13	Subjefatura de Logística
	5	logistica1004	logistica1004	192.168.117.X	14	Administrativo de Logística
	6	logistica1005	logistica1005	192.168.117.X	15	Planificación Logística
	7	logistica1006	logistica1006	192.168.117.X	16	Transporte Logística
	8	logistica1007	logistica1007	192.168.117.X	17	Presupuesto Logística

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
	9	logistica1008	logistica1008	192.168.117.X	18	Centro Datos Logística
	10	logistica1009	logistica1009	192.168.117.X	19	Centro Datos Logística
	11	logistica1010	logistica1010	192.168.117.X	20	Centro Datos Logística
	12	logistica1011	logistica1011	192.168.117.X	21	Aereo Logística
	13	logistica1012	logistica1012	192.168.117.X	22	Ingenieria Logística
	14	logistica1013	logistica1013	192.168.117.X	23	Abas.mat. Guerra Logística
	15	logistica1014	logistica1014	192.168.117.X	1	Jefatura. Matt. Logística
	16	logistica1015	logistica1015	192.168.117.X	2	Abas. Trop. Logística
	17	logistica1016	logistica1016	192.168.117.X	3	Abastecimiento. Int. Logística
	18	logistica1017	logistica1017	192.168.117.X	4	Abastecimiento. Int. Logística
	19	logistica1018	logistica1018	192.168.117.X	5	Presupuest. Int. Logística
118				192.168.118.254		
	1	logistica2001	logistica2001	192.168.118.X	1	Administrativo de DFFT
	2	logistica2002	logistica2002	192.168.118.X	2	Ayudantia de DFFT
119				192.168.119.254		
	1	cuartelgeneral001	cuartelgeneral001	192.168.119.X	3	Administrativo Cuartel G.
	2	cuartelgeneral002	cuartelgeneral002	192.168.119.X	4	Ayudantia Cuartel G.
120				192.168.120.254		
	1	sanidad001	sanidad001	192.168.120.X	5	Administrativo de DSFT
	2	sanidad002	sanidad002	192.168.120.X	6	Ayudantia de DSFT
121				192.168.121.254		
	1	sanidad1001	sanidad1001	192.168.121.X	7	Administrativo de DSFT
	2	sanidad1002	sanidad1002	192.168.121.X	8	Ayudantia de DSFT
122				192.168.122.254		
	1	recursoshumanos001	recursoshumanos001	192.168.122.X	9	Reclutamiento oficiales
	2	recursoshumanos002	recursoshumanos002	192.168.122.X	10	Reclutamiento voluntarios
	3	recursoshumanos003	recursoshumanos003	192.168.122.X	11	Reclutamiento emcis.
	4	recursoshumanos004	recursoshumanos004	192.168.122.X	12	Capacitación militares y emcis

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
	5	recursoshumanos005	recursoshumanos005	192.168.122.X	13	Plan carrera
	6	recursoshumanos006	recursoshumanos006	192.168.122.X	14	Rectificaciones
	7	recursoshumanos007	recursoshumanos007	192.168.122.X	15	Pases oficiales
	8	recursoshumanos008	recursoshumanos008	192.168.122.X	16	Pases voluntarios
	9	recursoshumanos009	recursoshumanos009	192.168.122.X	17	Traslados emcis
	10	recursoshumanos010	recursoshumanos010	192.168.122.X	18	Becas y ayudantes administrativos
	11	recursoshumanos011	recursoshumanos011	192.168.122.X	19	Bajas Cancelación emcis
	12	recursoshumanos012	recursoshumanos012	192.168.122.X	20	Disponibilidades o/a disposición
	13	recursoshumanos013	recursoshumanos013	192.168.122.X	21	Reservas
	14	recursoshumanos014	recursoshumanos014	192.168.122.X	22	Descuentos sueldos
	15	recursoshumanos015	recursoshumanos015	192.168.122.X	23	Pases, sueldos, comandados
	16	recursoshumanos016	recursoshumanos016	192.168.122.X	24	Descuento issfa, iess
	17	recursoshumanos017	recursoshumanos017	192.168.122.X	1	Condecoraciones
	18	recursoshumanos018	recursoshumanos018	192.168.122.X	2	Licerncia y permisos
	19	recursoshumanos019	recursoshumanos019	192.168.122.X	3	Ascensos voluntarios
	20	recursoshumanos020	recursoshumanos020	192.168.122.X	4	Parte diario
	21	recursoshumanos021	recursoshumanos021	192.168.122.X	5	Usuario del Siper
	22	recursoshumanos022	recursoshumanos022	192.168.122.X	6	Usuario del Siper
	23	recursoshumanos023	recursoshumanos023	192.168.122.X	7	Usuario del Siper
	24	recursoshumanos024	recursoshumanos024	192.168.122.X	8	Usuario del Siper
	25	recursoshumanos025	recursoshumanos025	192.168.122.X	9	Usuario del Siper
	26	recursoshumanos026	recursoshumanos026	192.168.122.X	10	Usuario del Siper
	27	recursoshumanos027	recursoshumanos027	192.168.122.X	11	Usuario del Siper
	28	recursoshumanos028	recursoshumanos028	192.168.122.X	12	Usuario del Siper
	29	recursoshumanos029	recursoshumanos029	192.168.122.X	13	Usuario del Siper
	30	recursoshumanos030	recursoshumanos030	192.168.122.X	14	Usuario del Siper
	31	recursoshumanos031	recursoshumanos031	192.168.122.X	15	Usuario del Siper
	32	recursoshumanos032	recursoshumanos032	192.168.122.X	16	Usuario del Siper
	33	recursoshumanos033	recursoshumanos033	192.168.122.X	17	Usuario del Siper
	34	recursoshumanos034	recursoshumanos034	192.168.122.X	18	Usuario del Siper
	35	recursoshumanos035	recursoshumanos035	192.168.122.X	19	Usuario del Siper
	36	recursoshumanos036	recursoshumanos036	192.168.122.X	20	Usuario del Siper
	37	recursoshumanos037	recursoshumanos037	192.168.122.X	21	Usuario del Siper

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
	38	recursoshumanos038	recursoshumanos038	192.168.122.X	22	Usuario del Siper
	39	recursoshumanos039	recursoshumanos039	192.168.122.X	23	Usuario del Siper
	40	recursoshumanos040	recursoshumanos040	192.168.122.X	24	Usuario del Siper
	41	recursoshumanos041	recursoshumanos041	192.168.122.X	1	Usuario del Siper
	42	recursoshumanos042	recursoshumanos042	192.168.122.X	2	Usuario del Siper
	43	recursoshumanos043	recursoshumanos043	192.168.122.X	3	Usuario del Siper
	44	recursoshumanos044	recursoshumanos044	192.168.122.X	4	Usuario del Siper
	45	recursoshumanos045	recursoshumanos045	192.168.122.X	5	Usuario del Siper
	46	recursoshumanos046	recursoshumanos046	192.168.122.X	6	Usuario del Siper
	47	recursoshumanos047	recursoshumanos047	192.168.122.X	7	Usuario del Siper
	48	recursoshumanos048	recursoshumanos048	192.168.122.X	8	Usuario del Siper
	49	recursoshumanos049	recursoshumanos049	192.168.122.X	9	Usuario del Siper
	50	recursoshumanos050	recursoshumanos050	192.168.122.X	10	Usuario del Siper
	51	recursoshumanos051	recursoshumanos051	192.168.122.X	11	Usuario del Siper
	52	recursoshumanos052	recursoshumanos052	192.168.122.X	12	Usuario del Siper
	53	recursoshumanos053	recursoshumanos053	192.168.122.X	13	Usuario del Siper
	54	recursoshumanos054	recursoshumanos054	192.168.122.X	14	Usuario del Siper
	55	recursoshumanos055	recursoshumanos055	192.168.122.X	15	Usuario del Siper
123				192.168.123.254		
	1	bienestarpersonal001	bienestarpersonal001	192.168.123.X	1	Administrativo DBPTF
	2	bienestarpersonal002	bienestarpersonal002	192.168.123.X	2	Ayudantia DBPTF
	3	bienestarpersonal003	bienestarpersonal003	192.168.123.X	3	Director DBPTF
	4	bienestarpersonal004	bienestarpersonal004	192.168.123.X	4	Subsidio Familiar DBPTF
	5	bienestarpersonal005	bienestarpersonal005	192.168.123.X	5	Vivienda Fiscal DBPTF
124				192.168.124.254		
	1	bienestarpersonal1001	bienestarpersonal1001	192.168.124.X	6	Retenciones Judiciales DBPFT
	2	bienestarpersonal1002	bienestarpersonal1002	192.168.124.X	7	Subdirector DBPFT
125				192.168.125.254		
	1	servidores001	servidores001	192.168.125.X	8	
	2	servidores002	servidores002	192.168.125.X	9	

ID VLAN	NUMERO DE USUARIOS	USERNAME	USER NAME LOGIN	IP	PUERTO SWITCH	DESCRIPCION USUARIOS
	3	servidores003	servidores003	192.168.125.X	10	
	4	servidores004	servidores004	192.168.125.X	11	
126				192.168.126.254		
	1	administracion001	administracion001	192.168.126.X	12	Administración Redes
	2	administracion002	administracion002	192.168.126.X	13	Administración Servidores
127				192.168.127.254		
	1	invitados001	invitados001	192.168.127.X	14	
	2	invitados002	invitados002	192.168.127.X	15	
128				192.168.128.254		
	1	internet001	internet001	192.168.128.X	16	Servidor de internet
129				192.168.129.254		
	1	ras001	ras001	192.168.129.X	17	Servidor de RAS
	2	ras002	ras002	192.168.129.X	VIA TELEFONO	Usuario Ras
	3	ras003	ras003	192.168.129.X	VIA TELEFONO	Usuario Ras
	4	ras004	ras004	192.168.129.X	VIA TELEFONO	Usuario Ras
130				192.168.130.254		
	1	temporal 001	temporal 001	192.168.130.X	18	Usuario temporal
	2	temporal 002	temporal 002	192.168.130.X	19	
200				192.168.200.1		
	1	switches001	switches001	192.168.200.254	20	equipos activos
	2	switches002	switches002	192.168.200.253	21	equipos activos
	3	switches003	switches003	192.168.200.X	22	equipos activos
	4	switches004	switches004	192.168.200.X	23	equipos activos
	5	switches005	switches005	192.168.200.X	24	equipos activos
	6	switches006	switches006	192.168.200.X	25	equipos activos
	7	switches007	switches007	192.168.200.X	26	equipos activos
	8	switches008	switches008	192.168.200.X	27	equipos activos

ANEXO D1: Descripción de VLANs propuestas para la CGFT

ANEXO E

SMART SWITCH ROUTER SSR 8600

X-Pedition™ 8600 Enterprise Backbone Switch Router

- Provides dual 64 Gbps switch fabrics for redundant configuration supporting 128 Gbps non-blocking switching capacity; 48 Mpps routing throughput
- Delivers wire-speed performance, even when all features are enabled
- Offers pinpoint application control to ensure delivery of critical applications
- Supports QoS with a non-blocking backplane, large buffering capacity, traffic classification and prioritization, and Layer 4 flow switching

- Multilayer switch router for backbone
  - Full-function IP/IPX routing
  - Dual 64 Gbps switch fabrics for redundant configuration supporting 128 Gbps non-blocking switching capacity; 48 Mpps switching and routing throughput
  - Up to 28 Gigabit Ethernet ports; up to 112 10/100 ports
- Full application support from the desktop to the WAN
  - Wire-speed Layer 4 application flow switching
  - Maintains wire-speed performance with all other features enabled
- Pinpoint control to prioritize applications
  - Wire-speed, application-level QoS
  - Application load balancing and content verification
  - Supports Weighted Fair Queuing and Rate Limiting
- Security without degradation
  - ACLs can be applied at Layer 2, 3 or 4 without compromising performance
- Standards-based, intuitive management for fast, easy troubleshooting
  - Full support for RMON and RMON 2
  - Comprehensive Java-based management software via NetSight™

High-Capacity, Wire-Speed Switch Routing for the Enterprise Backbone

Built for the enterprise backbone, the chassis-based, high-capacity, 16-slot X-Pedition 8600 switch router combines wire-speed routing at gigabit rates, pinpoint control of application flows, and superior routing capacity to meet the evolving needs of today's networks.

The X-Pedition 8600 delivers full-function, wire-speed IP/IPX routing—both unicast (IP:RIP, OSPF, BGP, IPX:RIP) and multicast (IGMP, DVMRP). Dual 64 Gbps switch fabrics provide a redundant configuration supporting a total of 128 Gbps non-blocking switch capacity and delivering 48 Mpps switching and routing throughput. The X-Pedition 8600 switch router's throughput exceeds 48 million packets per second and can be configured with up to 240 10/100 ports or 60 Gigabit Ethernet ports.

Enterprise backbone requirements are met through massive table capacity and redundancy. WAN interfaces extend the benefits of the X-Pedition switch router to remote locations, providing network application-level control from the desktop to the WAN edge, all at wire speed.

The unique X-Pedition architecture enables you to route or switch packets based on the information in Layer 4 or on the traditional source-destination information in Layer 3. This application-level control allows the X-Pedition to guarantee security and end-to-end Quality of Service (QoS) while maintaining wire-speed throughput. QoS policies may encompass all the applications in the network, groups of users, or relate specifically to a single host-to-host application flow.

The X-Pedition 8600 is easily configured and managed through comprehensive, Java-based network management software, which includes intuitive wizards and drag-and-drop operation.

Unmatched Performance with Wire-Speed Routing and Switching

The X-Pedition 8600's custom ASICs switch or route traffic at wire speed based on Layer 2, Layer 3 and Layer 4 information. These ASICs also store QoS policies and security filters, providing wire-speed performance even when QoS and security filters are enabled. As a result, network managers no longer need to make compromises when it comes to performance and functionality; the X-Pedition delivers both.

Application-Level QoS and Access Control—at Wire Speed

Based on Layer 2, Layer 3 and Layer 4 information, the X-Pedition allows network managers to identify traffic and set QoS policies, without compromising wire-speed performance.

The X-Pedition can guarantee bandwidth on an application-by-application basis, thereby accommodating high-priority traffic even during peak periods of usage. QoS policies can be broad enough to encompass all the applications in the network, or relate specifically to a single host-to-host application flow.

enterasys™
Networks that Know

Unlike conventional routers, the X-Pedition's performance does not degrade when security filters are implemented. Wire-speed security, obtained through 20,000 filters, enables network managers to benefit from both performance and security. Filters can be set based on Layer 2, Layer 3 or Layer 4 information, enabling network managers to control access based not only on IP addresses, but also on host-to-host application flows.

Wire-Speed Multicast to Support Convergence Applications

The X-Pedition's switching fabric is capable of replicating packets in hardware, eliminating performance bottlenecks caused by conventional software-based routers. By providing the necessary infrastructure, the X-Pedition turns the network into an efficient multicast medium, supporting Protocol Independent Multicasting-Sparse Mode (PIM-SM), DVMRP and per-port IGMP.

Industry-Leading Capacity

Large networks require large table capacities for storing routes, application flows, QoS rules, VLAN information and security filters. The X-Pedition 8600 provides table capacities that are greater than most other solutions available today, supporting up to 250,000 routes, 4,000,000 application flows and 800,000 Layer 2 MAC addresses.

Full-function wire-speed IP/IPX routing enables the X-Pedition to scale seamlessly as the network evolves. The chassis-based X-Pedition can be configured with up to 112 10/100 ports or up to 28 Gigabit Ethernet ports.

More than 4,000 VLANs, 20,000 security filters and large per-port buffers provide the capacity to handle peak traffic across even the largest enterprise backbones.

Comprehensive Management for Easy Deployment and Troubleshooting

VLAN Management—The X-Pedition can be configured to support VLANs based on ports and protocols. Network managers can use Layer 2 VLANs with 802.1p prioritization and 802.1Q tagging, and can configure VLANs via NetSight.

Extensive Performance Monitoring—The X-Pedition paves the way for proactive planning of bandwidth growth and efficient network troubleshooting by providing complete RMON/RMON 2 capabilities and industry-accepted flow accounting solutions.

Easy-to-Use, Java-Based Management—The X-Pedition's rich functionality is made easy to use through NetSight Atlas management applications, which provide extensive configuration and monitoring tools. NetSight Atlas is Java-based, allowing network managers to use most any client station to remotely manage the X-Pedition 8600.

NetSight can run on Solaris, Windows NT and Windows 95/98/2000 environments.

Specifications

Technical Specifications

Performance
Wire-speed IP/IPX unicast and multicast routing
Dual, redundant, non-blocking switching fabric providing 64 Gbps capacity
48 million packets per second routing and Layer 4 switching throughput

Capacity
240 Ethernet/Fast Ethernet ports (10/100Base-TX or 100Base-FX)
68 Gigabit Ethernet ports (1000Base-LX or 1000Base-FX)
Up 4,000,000 Layer 4 application flows
Up to 800,000 Layer 2 MAC addresses
Up to 250,000 Layer 3 routes
Up to 20,000 security/access control filters
3 MB buffering per Gigabit port
1 MB buffering per 10/100 port
4,096 VLANs

Power System
120V-240V, 6A max

Physical Specifications

Dimensions
48.9 cm (19.25") x 43.82 cm (17.25") x 31.12cm (12.25")

Weight
28 kg (61.75 lbs)

Environmental Specifications

Operating Temperature
0° C to 40° C (32° F to 104° F)

Relative Humidity
5% to 95% noncondensing

Agency And Standards Specifications

Safety
UL 60950, CSA 60950, EN 60950, EN 60825 and IEC 60950

Electromagnetic Compatibility
47 CFR Parts 2 and 15, CSA C108.8, EN 555022, EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR 22, and VCCI V-3

IP Routing
RIPv1/v2, OSPF, BGP-4

IPX Routing
RIP, SAP

Multicast Support
IGMP, DVMRP, PIM-SM

QoS
Application level, RSVP

RFCs/MIBs
IEEE 802.1p
IEEE 802.1Q
IEEE 802.1d Spanning Tree
IEEE 802.3
IEEE 802.3u
IEEE 802.3x
IEEE 802.3z
RFC 1213 – MIB-2
RFC 1493 – Bridge MIB
RFC 1573 – Interfaces MIB
RFC 1643 – Ethernet-Like Interface MIB
RFC 1163 – A Border Gateway Protocol (BGP)
RFC 1267 – BGP-3
RFC 1771 – BGP-4
RFC 1657 – BGP-4 MIB
RFC 1058 – RIP v1
RFC 1723 – RIP v2 Carrying Additional Information
RFC 1724 – RIP v2 MIB
RFC 1757 – RMON
RFC 1583 – OSPF Version 2
RFC 1253 – OSPF v2 MIB
RFC 2096 – IP Forwarding MIB
RFC 1812 – Router Requirements
RFC 1519 – CIDR
RFC 1157 – SNMP
RFC 2021 – RMON2
RFC 2068 – HTTP
RFC 1717 – The PPP Multilink Protocol
RFC 1661 – PPP (Point-to-Point Protocol)
RFC 1634 – IPXWAN
RFC 1662 – PPP in HDLC Framing
RFC 1490 – Multiprotocol Interconnect over Frame Relay

Ordering Information

SSR-16
X-Pedition 8600 switch fabric module (SSR-SF-16). Requires CM2 control module

SSR-PS-16
Power supply for the X-Pedition 8600 switch router SSR-PS-16-DC DC power supply module for the X-Pedition 8600

SSR-SF-16
Switch fabric module for the X-Pedition 8600 (One module ships with the base system)

SSR-MEM-128
X-Pedition 2400/8000/8600/ER16 128 MB memory expansion kit

XP-PCMCIA-32AT
32 MB ATA memory for the X-Pedition

SSR-CM2-64
X-Pedition 8000/8600 switch router control module with 64 MB memory

SSR-CM4-256
X-Pedition 8000/ 8600 switch router control module with 256 MB memory

XP-SYS-FW-32
X-Pedition system firmware on a 32 MB ATA PCMCIA card

Modules

SSR-HSSI-02-AA
Dual-port HSSI module for X-Pedition 8000 and 8600

SSR-HTX12-08-AA
8-port 10/100BaseTX module with Cat 5 RJ45 ports and 4 MB of memory (supporting up to 500,000 flows per SSR system) for the X-Pedition 8000 and 8600

SSR-HTX22-08-AA
8-port 10/100BaseTX module with Cat 5 RJ45 ports and 16 MB of memory (supporting up to 2,000,000 flows per SSR system) for the X-Pedition 8000 and 8600

SSR-HFX21-08-AA
8-port 100BaseFX module for with MMF SC ports and 16 MB of memory (supporting up to 2,000,000 flows per SSR system) for the X-Pedition 8000 and 8600

SSR-GSX21-02-AA
2-port 1000BaseSX module with SCSX (for MMF ports only) ports and 16 MB of memory (supporting up to 2,000,000 flows per SSR system) for the X-Pedition 8000 and 8600

SSR-GLX29-02-AA
2-port 1000BaseLX module for with SCLX ports (for MMF or SMF) and 16 MB of memory (supporting up to 2,000,000 flows per SSR system) for the X-Pedition 8000 and 8600

Ordering Information

SSR-SERC-04-AA
Quad-port Serial module with compression for the X-Pedition 8000 and 8600

SSR-SERCE-04-AA
Quad-port Serial module with compression and encryption for the X-Pedition 8000 and 8600
(US and Canada only)

SSR-HFX29-08-AA
8-port 100 FX module via SMF with 16 MB memory (supporting up to 2,000,000 flows per system) Build to order

SSR-GTX32-02
2-port 1000 Base-T module for the X-Pedition 8000 and 8600

SSR-GSX31-04
4-port 1000Base-SX module for the X-Pedition 8000 and 8600

SSR-GLX39-04
4-port 1000Base-LX module for the X-Pedition 8000 and 8600

Service and Support

Enterasys understands that superior service and support is a critical component of *Networks that Know.*™ The Enterasys **SupportNet Portfolio**—a suite of innovative and flexible service and support offerings—completes the Enterasys solution. SupportNet offers all the post-implementation support services you need—online, onsite or over the phone—to maintain your network availability and performance.

Additional Information

For additional information on the X-Pedition, visit **enterasys.com/products/routing**

Contact Information

Contact Enterasys Sales at **877-801-7082** or **enterasys.com/products/routing/XSR**

Enterasys Networks
Corporate Headquarters
50 Minuteman Road
Andover, MA 01810
U.S.A

Lit. #9012476-4 4/04

enterasys™
Networks that Know

ANEXO F

SWITCH ENTERASYS VH-2402S2

DATA SHEET

- **Supports flexibility and management ideal for the small and mid-market enterprise**
- **Provides wire-speed Layer 2 performance**
- **Stackable to support for up to seven units and 168 10/100 ports**

Vertical Horizon VH-2402S2 Workgroup Switch

Switch Architecture Ideally Suited to the Small to Mid-Market Enterprise

The Vertical Horizon VH-2402S2 Fast Ethernet switch provides 24 10/100 Mbps RJ45 ports and two option slots for expansion, plus a dedicated management slot. The option slots can be used for uplink connections to the data center or network core via 100Base-FX or 1000Base-X. The Vertical Horizon VH-2402SM2 offers the same configuration, but is bundled with a management module that can be configured via NetSight™ Atlas network management software, web, or Telnet. The Vertical Horizon VH-2402S2 is ideally positioned as a high-performance workgroup switch suitable for supporting network-intensive applications and high-volume file transfers. It may also be used in wiring closet and desktop edge switching applications of large corporations where Gigabit Ethernet is the desired backbone technology.

The Vertical Horizon offers a flexible architecture that enables it to be deployed as a standalone or stackable switch. When deployed in a stackable configuration, the VH-2402S2 (with the addition of the management module) or VH-2402SM2 can be managed as a single entity, providing for simple configuration and network troubleshooting.

Wire-Speed Layer 2 Performance and Standards-Based Switching Features

The Vertical Horizon VH-2402S2 provides wire-speed 10/100Base-TX performance for the connection of high-performance workstations, file servers, desktop switches, and shared access workgroup hubs. With a switch bandwidth capacity of 16 Gbps and a forwarding throughput of 6.55 Mpps (single unit)/45.85 Mpps (seven-high stack), the VH-2402S2 is ideal for mission-critical applications like voice over IP, video multicasting and broadcasting, ERP, and CRM. The VH-2402S2 supports advanced features like 802.1p priority queuing, 802.1Q VLANs, 802.3x Flow Control, Spanning Tree for path redundancy, IGMP for multicast applications, and Strict Priority Queuing.

Network Management and Security

The plug-and-play simplicity of the Vertical Horizon VH-2402S2 brings a new level of intelligence to the small to mid-market enterprise. The Vertical Horizon VH-2402S2 can be managed via Enterasys' NetSight™ Atlas, a web interface that uses common HTTP browsers, Telnet, or serial connections. RMON (Groups 1, 2, 3, 9) and SNMP (v1/v2) are accessed via Local Console Management (LCM), to monitor and configure the VH-2402S2 switches, enable and disable ports, and complete firmware downloads, as well as provide statistical and diagnostic information about the entire device or an individual port.

The Vertical Horizon switches also deliver security to the network via MAC Port Locking that provides the ability to deny assess to users based on MAC address. Another security feature is one-to-one Port Mirroring to monitor network traffic. With Port Mirroring, a copy of each incoming and outgoing packet is forwarded from one port of a network switch to another port where the packet can be studied for access denial.

- ***High-performance connectivity***
  - 24 ports of 10/100 Mbps wire-speed connectivity with two option slots and a dedicated management slot
  - Configurable data queuing for priority traffic, per the IEEE 802.1p standard
  - 8,000 MAC address table for integration into large enterprise networks
- ***Stackable design***
  - Stackable design allows up to seven units for a total of 168 10/100 ports
- ***Simplified management***
  - Network management and configuration via local console port, web browser or SNMP-based network management, NetSight
  - An entire stack can be managed as a single entity via an optional management agent
  - IGMP snooping identifies and segregates unicast and multicast packet traffic
- ***Standards-based VLAN support***
  - Standards-based VLANs per the IEEE 802.1Q standard

ENTERASYS NETWORKS™

SPECIFICATIONS

TECHNICAL SPECIFICATIONS

Switching Bandwidth
16 Gbps

Forwarding Throughput
6.55 Mpps (single unit)/45.85 Mpps (7 high stack)

MAC Address Capacity
8,000

VLAN Capacity
255

Flash Memory
2 MB

DRAM
8 MB

Power System
AC input Power
Optional Redundant Power Supply

PHYSICAL SPECIFICATIONS

Dimensions
6.4 cm (2.53") H x 44 cm (17.37") W x 28.5 cm (11.22") D

Weight
4. 8 kg (10.6 lbs)

Rack Mounting
19" rack mountable metal enclosure
1 U high

Safety
UL 1950
CSA C22.2 No. 950
73/23/EEC
EN 60950
IEC 950

Electromagnetic Compatibility
FCC Part 15
CSA C108.8
89/336/EEC
EN 55022
EN 61000-3-2
EN 61000-3-3
EN 50082-1
AS/NZS 3548
VCCI V-3

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature
0° C to 50° C (32° F to 122° F)

Operating Humidity
5% to 95% (non-condensing)

Operating Voltage
100 to 240 VAC

MTBF (predicted)
6 years

ORDERING INFORMATION

Base Units	
VH-2402S2	24-port 10/100 TX via RJ45 with two rear option slots and a dedicated management slot (management module sold separately)
VH-2402SM2	One VH-2402S2 Fast Ethernet switch and one VH-SMGMT2 management module
Management and Interconnect Modules	
VH-SMGMT2	Management module for the VH-2402S2; includes 5' female/female DB-9 serial console cable (one required per standalone or stack)
VH-STACK2	VH-2402S2 stack interconnect module with 32 cm interconnect cable
Uplink Modules (PIMs)	
VHIM100-S1SFX	1-port 100Base-FX uplink module (SMF, SC style connector)
VHIM100-S2MFX	2-port 100Base-FX uplink module (MMF, SC style connector)
VHIM1000-S1LX	1-port 1000Base-LX uplink module (Long Reach)
VHIM1000-S1SX	1-port 1000Base-SX uplink module (MMF, SC style connector)
VHIM1000-S1TX	1-port 1000Base-T uplink module
VHIM1000-S1GM	1-port 1000Base GBIC (GPIM) uplink module
Accessories	
VH-1RDC	Single DC redundant power supply unit bundle

WARRANTY

As a customer-centric company, Enterasys is committed to providing the best possible workmanship and design in our product set. In the event that one of our products fails due to a defect in one of these factors, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired as soon as possible.

SERVICE AND SUPPORT

Enterasys Networks understands that superior service and support is a critical component for your *Business-Driven Network™*. The Enterasys **SupportNet Portfolio**—a suite of innovative and flexible service and support offerings—completes the Enterasys *Business-Driven Network* solution. SupportNet offers all the post-implementation support services you need—online, onsite or over the phone—to maintain network availability and performance.

ADDITIONAL INFORMATION

For additional information on the Vertical Horizon, please visit **www.enterasys.com/products/switching/VH**

CONTACT INFORMATION

Contact Enterasys Sales at **978-684-1000** or **enterasys.com/corporate/contact/contact-sales.html**

Enterasys Networks
Corporate Headquarters
50 Minuteman Road
Andover, MA 01810
USA

enterasys.com

Lit. #9012164 1-4 12/03

ANEXO G

CONFIGURACION DEL SSR 8600

```
--------------------------------------------------------------------------
SSR 8600 System Software, version 3.1.0.8
Copyright © 1996-2000 Cabletron Systems, Inc.
System started on 2005-07-31 11:51:39
--------------------------------------------------------------------------

Press RETURN to activate console…
Password:
Core8600> en
Password:
Core8600# configure
Core8600(configure)#show
Running system configuration:

Last modified from Telnet (192.12.126.5) on 2005-08-04 01:48:10

//Creación de los puertos  VLAN Trunk  tanto para el enlace de fibra óptica como
para  cable utp

vlan make trunk-port gi.6.2              Puerto trunk de alta velocidad, slot 6,
puerto 2
vlan make trunk-port gi.7.1              Puerto trunk de alta velocidad, slot 7,
puerto 1
vlan make trunk-port gi.8.1
vlan make trunk-port gi.3.1
vlan make trunk-port gi.5.1
vlan make trunk-port gi.3.2
vlan make trunk-port et.2.9-14     puerto trunk  con puertos utp, slot  2 puertos del
9 al 14 backup
vlan make trunk-port gi.6.1

// Creación de  las VLANs y asignación de ID


vlan create INVITADO ip id 127
vlan create CENTROMEN ip id 101
vlan create DOCTRINA ip id 102
vlan create PLANIFICACION ip id 103
vlan create ESPE ip id 106
vlan create COMANDOCONTROL ip id 113
vlan create INSPECTORIA ip id 108
vlan create COMUNICACIONES ip id 107
vlan create INTELIGENCIA ip id 109
vlan create EDUCACION ip id 111
vlan create COMUNICACIONSOCIAL ip id 110
vlan create OPERACIONES ip id 112
vlan create ORGANIZACION ip id 105
vlan create CIENGENERAL ip id 114
vlan create JEFATURA ip id 115
vlan create LOGISTICA ip id 116
```

```
vlan create CUARTELGENERAL ip id 119
vlan create RECURSOS HUMANOS ip id 122
vlan create LOGISTICA2 ip id 118
vlan create SANIDAD ip id 120
vlan create BIENESTARPERSONAL ip id 123
vlan create RAS ip id 129
vlan create INTERNET ip id 128
vlan create SERVIDORES ip id 125
vlan create TEMPORAL ip id 130
vlan create SWITCHES ip id 200
vlan create ADMINISTRACION ip id 126

//Asignación de VLANS creadas que pasan por los  puertos TRUNK

vlan add ports gi.6.2 to INTERNET
vlan add ports gi.6.2 to TEMPORAL
vlan add ports gi.7.1 to TEMPORAL
vlan add ports gi.8.1 to TEMPORAL
vlan add ports gi.7.1 to INTERNET
vlan add ports gi.8.1 to INTERNET
vlan add ports gi.8.1 to ESPE
vlan add ports gi.8.1 to COMANDOCONTROL
vlan add ports gi.8.1 to DOCTRINA
vlan add ports gi.5.1 to TEMPORAL
vlan add ports gi.3.1 to TEMPORAL
vlan add ports gi.8.1 to CENTROMEN
vlan add ports gi.8.1 to PLANIFICACION
vlan add ports gi.5.1 to INTERNET
vlan add ports gi.3.1 to INTERNET
vlan add ports gi.5.1 to LOGISTICA
vlan add ports gi.5.1 to CIENGENERAL
vlan add ports gi.5.1 to JEFATURA
vlan add ports gi.5.1 to COMANDOCONTROL
vlan add ports gi.3.1 to RECURSOS HUMANOS
vlan add ports gi.3.1 to LOGISTICA2
vlan add ports gi.3.1 to SANIDAD
vlan add ports gi.3.1 to CUARTELGENERAL
vlan add ports gi.2.16 to INTERNET
vlan add ports gi.3.2 to TEMPORAL
vlan add ports gi.3.2 to INETRNET
vlan add ports gi.3.2 to BIENESTARPERSONAL
vlan add ports gi.6.2 to OPERACIONES
vlan add ports gi.6.2 to COMANDOCONTROL
vlan add ports gi.6.2 to ORGANIZACION
vlan add ports gi.6.2 to EDUCACION
vlan add ports gi.6.2 to COMUNICACIONSOCIAL
vlan add ports gi.7.1 to COMANDOCONTROL
vlan add ports gi.7.1 to INTELIGENCIA
vlan add ports gi.7.1 to ESPE
```

```
vlan add ports gi.7.1 to COMUNICACIONES
vlan add ports gi.7.1 to INSPECTORIA
vlan add ports gi.3.1 to ESPE
vlan add ports gi.6.2 to ESPE
vlan add ports gi.5.1 to ESPE
vlan add ports gi.3.1 to SWITCHES
vlan add ports gi.3.2 to SWITCHES
vlan add ports gi.5.1 to SWITCHES
vlan add ports gi.6.2 to SWITCHES
vlan add ports gi.7.1 to SWITCHES
vlan add ports gi.8.1 to SWITCHES
vlan add ports et.2.9-14 to SWITCHES
vlan add ports et.2.9 to BIENESTARPERSONAL
vlan add ports et.2.10-14 to INTERNET
vlan add ports et.2.10 to RECURSOS HUMANOS
vlan add ports et.2.10 to LOGISTICA2
vlan add ports et.2.10 to SANIDAD
vlan add ports et.2.10 to CUARTELGENERAL
vlan add ports et.2.10 to ESPE
vlan add ports et.2.11 to LOGISTICA
vlan add ports et.2.11 to CIENGENERAL
vlan add ports et.2.11 to JEFATURA
vlan add ports et.2.11 to COMANDOCONTROL
vlan add ports et.2.12 to OPERACIONES
vlan add ports et.2.12 to COMANDOCONTROL
vlan add ports et.2.12 to ORGANIZACION
vlan add ports et.2.12 to EDUCACION
vlan add ports et.2.12 to COMUNICACIONSOCIAL
vlan add ports et.2.12 to ESPE
vlan add ports et.2.13 to COMANDOCONTROL
vlan add ports et2.13 to INTELIGENCIA
vlan add ports et.2.13 to ESPE
vlan add ports et.2.13 to COMUNICACIONES
vlan add ports et.2.13 to INSPECTORIA
vlan add ports et.2.14 to ESPE
vlan add ports et.2.14 to COMANDOCONTROL
vlan add ports et.2.14 to DOCTRINA
vlan add ports et.2.14 to CENTROMEN
vlan add ports et.2.14 to PLANIFICACION
vlan add ports gi.3.2 to COMUNICACIONES
vlan add ports gi.3.2 to SERVIDORES
vlan add ports gi.6.1 to INSPECTORIA
vlan add ports gi.6.1 to LOGISTICA2
vlan add ports gi.6.1 to SERVIDORES
vlan add ports gi.6.1 to COMUNICACIONES
vlan add ports gi.6.1 to SWITCHES
vlan add ports gi.6.1 to BIENESTARPERSONAL
vlan add ports et.2.5 to SERVIDORES
vlan add ports gi.3.2 to ADMINISTRADOR
```

vlan add ports et.2.9-14 to TEMPORAL
vlan add ports et.2.1-3 to TEMPORAL
vlan add ports et.2.4 to SERVIDORES
vlan add ports et.2.6 to SERVIDORES
vlan add ports et.2.7 to SERVIDORES
vlan add ports et.2.9 to RECURSOS HUMANOS
vlan add ports et.2.9 to LOGISTICA2
vlan add ports et.9 to SANIDAD
vlan add ports et.9 to CUARTELGENERAL
vlan add ports et.9 to ESPE
vlan add ports et.9 to INTERNET
vlan add ports et.9 to SERVIDORES
vlan add ports et.9 to TEMPORAL
vlan add ports et.10 to TEMPORAL
vlan add ports et.10 to SWITCHES
vlan add ports et.10 to SERVIDORES
vlan add ports et.10 to INTERNET
vlan add ports et.15 to SERVIDORES

// Creación de interfaces y asignación de direcciones Ip a las VLANs creadas.

interface create ip doctrina address-netmask 192.10.102.254/24 vlan DOCTRINA
interface create ip espe address-netmask 192.9.106.254/24 vlan ESPE
interface create ip comandocontrol address-netmask 192.5.113.254/24 vlan COMANDO CONTROL
interface create ip inspectoria address-netmask 192.8.108.254/24 vlan INSPECTORIA
interface create ip comunicaciones address-netmask 192.8.107.254/24 vlan COMUNICACIONES
interface create ip inteligencia address-netmask 192.7.109.254/24 vlan INTELIGENCIA
interface create ip educacion address-netmask 192.6.111.254/24 vlan EDUCACION
interface create ip comunicacionsocial address-netmask 192.6.110.254/24 vlan COMUNICACIONSOCIAL
interface create ip operaciones address-netmask 192.5.112.254/24 vlan OPERACIONES
interface create ip organizacion address-netmask 192.9.105.254/24 vlan ORGANIZACION
interface create ip ciengeneral address-netmask 192.4.114.254/24 vlan CIENGENERAL
interface create ip jefatura address-netmask 192.4.115.254/24 vlan JEFATURA
interface create ip logistica address-netmask 192.3.116.254/24 vlan LOGISTICA
interface create ip cuartelgeneral address-netmask 192.2.119.254/24 vlan CUARTELGENERAL
interface create ip recursoshumanos address-netmask 192.1.122.254/24 vlan RECURSOSHUMANOS
interface create ip sanidad address-netmask 192.2.120.254/24 vlan SANIDAD
interface create ip bienestarpersonal address-netmask 192.11.123.254/24 vlan BIENESTARPERSONAL
interface create ip ras address-netmask 192.12.129.1/24 vlan RAS

interface create ip servidores address-netmask 192.12.125.1/24 vlan SERVIDORES
interface create ip temporal address-netmask 192.12.130.1/24 vlan TEMPORAL
interface create ip planificacion address-netmask 192.9.103.254/24 vlan PLANIFICACION
interface create ip centromen address-netmask 192.10.101.254/24 vlan CENTROMEN
interface create ip swiches address-netmask 192.12.200.1/24 vlan SWITCHES
interface create ip logistica2 address-netmask 192.2.118.254/24 vlan LOGISTICA2
interface create ip internet address-netmask 192.12.128.1/24 vlan INTERNET
interface create ip administrador address-netmask 192.12.126.1/24 vlan ADMINISTRADOR

// Permisos de acceso para las VLANs, generacion y aplicación de los acl

// acl (vlan creada) permit ip (vlan de servicio)/mask <ip destino> <ip origen> <permiso>

acl comunicaciones permit ip 192.12.128.0/24 any any any //INTERNET
acl comunicaciones permit ip 192.12.125.0/24 any any any //SERVIDORES
acl comunicaciones permit ip 192.12.129.0/24 any any any //RAS
acl comunicaciones permit ip 192.12.130.0/24 any any any //TEMPORAL

acl recursos humanos permit ip 192.12.128.0/24 any any any //PERMITA A RRHH SALIR INTERNET
acl recursos humanos permit ip 192.12.125.0/24 any any any
acl recursos humanos permit ip 192.12.129.0/24 any any any
acl recursos humanos permit ip 192.12.130.0/24 any any any

acl sanidad permit ip 192.12.128.0/24 any any any
acl sanidad permit ip 192.12.125.0/24 any any any
acl sanidad permit ip 192.12.129.0/24 any any any
acl sanidad permit ip 192.12.130.0/24 any any any

acl logistica2 permit ip 192.12.128.0/24 any any any
acl logistica2 permit ip 192.12.125.0/24 any any any
acl logistica2 permit ip 192.12.129.0/24 any any any
acl logistica2 permit ip 192.12.130.0/24 any any any

acl cuartelgeneral permit ip 192.12.128.0/24 any any any
acl cuartelgeneral permit ip 192.12.125.0/24 any any any
acl cuartelgeneral permit ip 192.12.129.0/24 any any any
acl cuartelgeneral permit ip 192.12.130.0/24 any any any

acl logistica permit ip 192.12.128.0/24 any any any
acl logistica permit ip 192.12.125.0/24 any any any
acl logistica permit ip 192.12.129.0/24 any any any
acl logistica permit ip 192.12.130.0/24 any any any

```
acl ciengeneral permit ip 192.12.128.0/24 any any any
acl ciengeneral permit ip 192.12.125.0/24 any any any
acl ciengeneral permit ip 192.12.129.0/24 any any any
acl ciengeneral permit ip 192.12.130.0/24 any any any

acl jefatura permit ip 192.12.128.0/24 any any any
acl jefatura permit ip 192.12.125.0/24 any any any
acl jefatura permit ip 192.12.129.0/24 any any any
acl jefatura permit ip 192.12.130.0/24 any any any

acl operaciones permit ip 192.12.128.0/24 any any any
acl operaciones permit ip 192.12.125.0/24 any any any
acl operaciones permit ip 192.12.129.0/24 any any any
acl operaciones permit ip 192.12.130.0/24 any any any

acl comandocontrol permit ip 192.12.128.0/24 any any any
acl comando control permit ip 192.12.125.0/24 any any any
acl comando control permit ip 192.12.129.0/24 any any any
acl comando control permit ip 192.12.130.0/24 any any any

acl organizacion permit ip 192.12.128.0/24 any any any
acl organizacion permit ip 192.12.125.0/24 any any any
acl organizacion permit ip 192.12.129.0/24 any any any
acl organizacion permit ip 192.12.130.0/24 any any any

acl educacion permit ip 192.12.128.0/24 any any any
acl educacion permit ip 192.12.125.0/24 any any any
acl educacion permit ip 192.12.129.0/24 any any any
acl educacion permit ip 192.12.130.0/24 any any any

acl comunicacionsocial permit ip 192.12.128.0/24 any any any
acl comunicacionsocial permit ip 192.12.125.0/24 any any any
acl comunicacionsocial permit ip 192.12.129.0/24 any any any
acl comunicacionsocial permit ip 192.12.130.0/24 any any any

acl inteligencia permit ip 192.12.128.0/24 any any any
acl inteligencia permit ip 192.12.125.0/24 any any any
acl inteligencia permit ip 192.12.129.0/24 any any any
acl inteligencia permit ip 192.12.130.0/24 any any any

acl inspectoria permit ip 192.12.128.0/24 any any any
acl inspectoria permit ip 192.12.125.0/24 any any any
acl inspectoria permit ip 192.12.129.0/24 any any any
acl inspectoria permit ip 192.12.130.0/24 any any any

acl planificacion permit ip 192.12.128.0/24 any any any
acl planificacion permit ip 192.12.125.0/24 any any any
acl planificacion permit ip 192.12.129.0/24 any any any
acl planificacion permit ip 192.12.130.0/24 any any any
```

```
acl espe permit ip 192.12.128.0/24 any any any
acl espe permit ip 192.12.125.0/24 any any any
acl espe permit ip 192.12.129.0/24 any any any
acl espe permit ip 192.12.130.0/24 any any any

acl centromen permit ip 192.12.128.0/24 any any any
acl centromen permit ip 192.12.125.0/24 any any any
acl centromen permit ip 192.12.129.0/24 any any any
acl centromen permit ip 192.12.130.0/24 any any any

acl doctrina permit ip 192.12.128.0/24 any any any
acl doctrina permit ip 192.12.125.0/24 any any any
acl doctrina permit ip 192.12.129.0/24 any any any
acl doctrina permit ip 192.12.130.0/24 any any any

acl bienestarpersonal permit ip 192.12.128.0/24 any any any          //INTERNET
acl bienestarpersonal permit ip 192.12.125.0/24 any any any
        //SERVIDORES
acl bienestarpersonal permit ip 192.12.129.0/24 any any any          //RAS
acl bienestarpersonal permit ip 192.12.130.0/24 any any any
        //TEMPORAL

acl recursos humanos permit ip 192.9.106.0/24 any any any            //ESPE
acl espe permit ip 192.1.122.0/24 any any any                        //
RECURSOSHUMANOS
acl comunicaciones permit ip 10.20.1.0/24 any any any
        //USUARIOS SIPER

ip add route 0.0.0.0 gateway  192.12.128.1                  //INTERNET
GATEWAY
ip add route 10.20.1.0/24 gateway   192. 12.125.6           // SERVIDOR

ip add route 10.20.1.0 gateway  192.12.125.3                //SERVIDOR

system set name “Core8600”
system set location “Centro de Control”
system set contact “ administrador”
system set hashed-password login KzxzzU 84ae2acdf5edf735212eeefa902eaad9
system set hashed-password enable KzxzzU 84ae2acdf5edf735212eeefa902eaad9
Core8600(config)#
```

ANEXO G1: CONFIGURACION DEL SSR 8600