Reingeniería de la Red de Datos de un Ente del Ministerio de Defensa Nacional (MIDENA) (Marzo 2012)

Nancy Yolanda Ramón Ibujés

Director: Ing. Carlos Vásquez

***Resumen*—El presente trabajo plantea un diseño que permite mejorar el desempeño de la red, proponiendo un esquema basado en un estudio pormenorizado de su infraestructura y requerimientos actuales, mediante la aplicación de un modelo jerárquico basado en el estudio por capas y la microsegmentación a nivel lógico de la red, además de la implementación de un esquema que asegura la continuidad del servicio. Con el desarrollo de la simulación se demuestra la funcionalidad del modelo previamente establecido mediante la utilización del software Packet Tracer 5.3.1 el cual brinda una interfaz que facilita validar las configuraciones realizadas, demostrando su operatividad en independencia de la tecnología de infraestructura utilizada.**

La elaboración del presente proyecto brinda una solución eficiente para la red de Datos de la Institución bajo la cual se mejora las prestaciones y el servicio ofrecido tanto hacia los diferentes entes asociados como hacia la red interna, considerando la infraestructura actual con la que cuenta la misma.

I. Introducción

El Ministerio de Defensa Nacional es la instancia político administrativa del Poder Ejecutivo, que se encarga de dirigir la Política de Defensa y administrar las Fuerzas Armadas armonizando sus acciones entre las funciones del Estado y la Institución Militar.

Dentro del marco Nacional las Fuerzas Armadas deben conjugar sus acciones con el Desarrollo Social, Nacional e Internacional, además de contrastar con el avance de la ciencia y tecnología que le permita enfrentar los nuevos retos, riesgos y amenazas en Pro de los Intereses Nacionales.

En este contexto el Ente del Ministerio de Defensa Nacional en estudio, es uno de los organismos de planificación y dirección militar cuya estructura interna debe permitir una rápida acción ante la toma de decisiones trascendentales en beneficio de todos los habitantes de la nación, protegiendo su soberanía.

Debido a las características de los servicios, es necesario que la red cuente con alta disponibilidad y calidad de servicio por medio de una infraestructura de red que soporte grandes cantidades de tráfico, además de poseer escalabilidad y flexibilidad.

Para el desarrollo del diseño de red que cumpla con los factores indicados, es necesario que se desarrollen varias etapas previas, con las cuales en primera instancia se conozca la situación actual de la red para luego proceder al desarrollo de un diseño que se ajuste a sus necesidades y cumpla con sus requerimientos.

II. Análisis de la situación actual de la red de datos

Con el fin de determinar el estado actual de la red de datos se realiza un estudio situacional, el cual muestre los requerimientos referentes a servicios y seguridad de la red.

El desarrollo del levantamiento de red involucra aspectos claves como: cableado estructurado, estructura física y lógica de la red, cantidad de usuarios y su función dentro de cada departamento, ubicación y estado de puntos de red, comportamiento del espectro electromagnético dentro de las instalaciones, además de los elementos que conforman la parte activa de la red; es decir su estudio debe reflejar a detalle su estado situacional.

El Cableado Estructurado constituye la base fundamental para la prestación de servicios de red, por lo cual es importante que éste se encuentre en perfecto estado.

Dentro del levantamiento de información del cableado estructurado se deben considerar los siguientes elementos: cableado horizontal, cableado vertical, área de trabajo, cuarto de telecomunicaciones y cuarto de equipos, cuarto de entrada de servicios y sistema de puesta a tierra. Además del levantamiento de cada uno de los elementos descritos, de debe identificar el cumplimiento de las normas y estándares de cableado estructurado, con lo cual podamos asegurar primero la conexión y posteriormente la comunicación en la red.

Dependiendo de la antigüedad de los sistemas de cableado es meritorio realizar una certificación del cableado

estructurado, de manera que se determine su estado y rendimiento; la certificación de los puntos de red determina el cumplimiento o incumplimientos de los parámetros de red y a su vez se valida el cumplimiento de normas y estándares de CE[1] basados en el TSB[2]67. En base al informe de certificación se puede definir la operatividad del sistema de cableado estructurado o dar la justificación para el cambio del mismo, dado que no brinde las características que aseguren la comunicación en relación a la demanda de los servicios ofrecidos por la institución.

Estructura física y lógica.- El levantamiento de la infraestructura de red implica además de ubicar todos los elementos activos de la red, determinar su modelo de conexión, además de levantar la configuración de cada uno de los equipos, de manera que se identifique la topología a nivel lógico manejada en la infraestructura de red de la institución.

El diagrama de la topología de red permite identificar de manera clara la situación de la red desde una perspectiva operativa, es importante que su análisis se divida en al menos dos partes: una vista de la perspectiva externa o de internet y otra desde la perspectiva interna o la intranet con sus elementos constituyentes. La vista interna puede subdividirse en función de las redes que se manejen en su interior de manera que se pueda puntualizar su levantamiento, identificando el equipamiento de red, conexiones entre los mismos y principalmente los problemas de seguridad asociados. Con la topología lógica se identifica la segmentación de red utilizada, posibles cuellos de botella de la red, dominios de broadcast, rutas críticas, entre otros.

Con el análisis de las configuraciones del equipamiento de red además se puede determinar los problemas de seguridad en su configuración, principalmente asociados al uso de contraseñas, protocolos de acceso no seguros y configuraciones innecesarias.

En toda la infraestructura de red es importante que se mantenga actualizadas dichas topologías, dado que las mismas permiten identificar de manera gráfica la estructura de red de manera que se cuente con una herramienta de fácil observación y análisis para permitir una rápida acción ante la toma de decisiones.

Espectro electromagnético.- El estudio del espectro electromagnético permite identificar la utilización del espectro permitiendo determinar los canales ocupados y su disponibilidad ó saturación, además del cumplimiento de estándares. Es importante que antes de incluir nuevos canales en operación se realice un estudio que indique su disponibilidad de manera que se evite el solapamiento de señales a causa del uso indebido de los mismos, además es importante que para tener un ambiente en operación óptimo, se respete la separación de canales establecido en las normas IEEE[3] 802.11 b, g.

[1]CE: Cableado estructurado

[2] TSB: Technical Service Bulletin (Boletín Técnico de Servicio)

[3] IEEE: The Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)

Levantamiento a nivel de usuario final.- la determinación de los usuarios existentes en la red junto con su ubicación, función y requerimientos, permite conocer a detalle los elementos constituyentes en una red, así como las necesidades de la misma. Es importante tener en cuenta los recursos compartidos en la red, parámetros determinantes para el establecimiento de un modelo funcional de manera que no se vean afectadas las actividades de los usuarios.

Al igual que las topologías de red, el levantamiento a nivel de usuario final junto con sus componentes, debe ser constantemente actualizado y claramente identificado, este documento será utilizado por el administrador como un documento de apoyo, que además facilitará la identificación de fallas.

El éxito de un diseño de red depende de la etapa de levantamiento de información dentro de la cual se obtiene toda la información que sirve como base para el desarrollo de las siguientes etapas. Durante el análisis de la información en cambio se determina los requerimientos y necesidades a tomarse en cuenta en el diseño de la red, así como los criterios a tomarse en cuenta para su diseño, de manera que el diseño sea funcional para la red de la institución.

III. DISEÑO DE TOPOLOGÍAS FÍSICA Y LÓGICA

Dentro del diseño de las topologías de red se especifican los parámetros más relevantes a tomarse en cuenta para la implementación del modelo. Sin embargo antes de empezar con el planteamiento del diseño es importante tener en cuenta tres aspectos como son: la proyección de crecimiento a nivel de usuarios en la red, políticas aplicadas y el análisis de los requerimientos de los usuarios.

Teniendo en cuenta la proyección de crecimiento estimado de la red, su diseño debe ajustarse a los requerimientos con una infraestructura completamente operativa en función de su crecimiento, teniendo en cuenta también la demanda de equipos que esto implique. Las políticas de red predefinidas en la institución en cambio brindan los principales lineamientos de seguridad, así como la regulación del uso de las instalaciones, equipamiento y servicios de la misma que deben observarse. Para que el diseño realizado sea funcional debe tenerse en cuenta además los requerimientos de los usuarios obtenidos durante el levantamiento de información, como necesidad de adición de puntos de red, uso de recursos compartidos, entre otros.

A. Reingeniería de la red de datos

Luego de realizado el análisis de la información referente al estudio situacional de la red de la institución y conociendo su estructura interna, se plantea el rediseño de la red de datos, partiendo de su estructura lógica y física estudiada, la cual provea una red escalable, flexible, fácilmente administrable, además de disponible, que reduzca el tamaño de los dominios de broadcast existentes, permitiendo una solución integral para la red de datos.

El diseño debe permitir mejorar el rendimiento de la red al aprovechar óptimamente el equipamiento existente con una

administración adecuada, efectuando cambios drásticos sobre la misma.

La reingeniería de red parte del análisis de diseño a nivel de cableado estructurado, el mismo que está basado en el cumplimiento de las normas ANSI[4]/TIA[5]/EIA[6]-568-B, ANSI/TIA/EIA-569, ANSI/TIA/EIA-606-A y ANSI/TIA/EIA-J-STD-607-A.

1) Modelo de red

La solución de rediseño para la red de datos de la institución debe permitir que la red sea fácilmente administrable, con facilidad de expansión, disponible, segura y con la capacidad de resolver los problemas con rapidez; estas características son brindadas por un modelo de red del tipo jerárquico.

El modelo citado está basado en el diseño y estructuración por capas dentro del cual cada una de ellas tiene su función y rol específico en la red, de esta manera se diferencian tres capas:

- núcleo
- distribución y
- acceso.

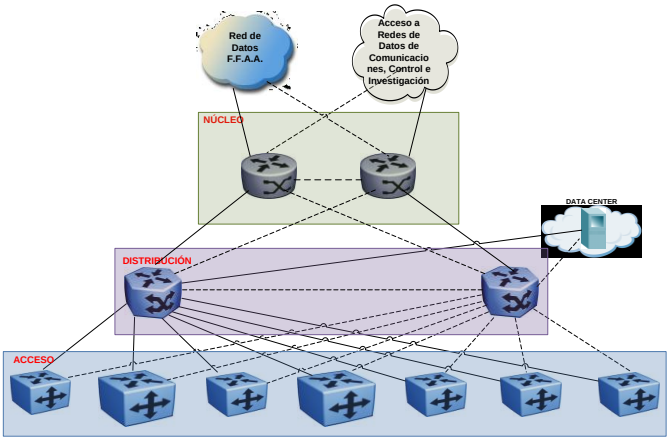

Fig. 1. Modelo General de Red

En la figura se observa de manera general el modelo de red planteado para la institución, en base al cual para cada una de las capas se define su funcionalidad, equipamiento y características propias de cada una de ellas.

Dentro de las ventajas del modelo se destacan las siguientes:

- **Escalabilidad:** fácil crecimiento y expansión, su crecimiento se realiza desde el nivel de acceso hacia el nivel de núcleo, según la necesidad y la disponibilidad de puertos.
- **Rendimiento:** los switches de núcleo y distribución al tener buenas características manejan grandes velocidades, evitando tener cuellos de botella en la red.
- **Seguridad:** se permite manejar políticas tanto en los switches del nivel de distribución como en los de nivel de acceso permitiendo establecer políticas hasta a nivel de puerto.
- **Redundancia:** permite tener alta disponibilidad en la red, evitando tener caídas de servicio en la misma.
- **Aislamiento de fallas:** permite aislar equipos defectuosos de manera que no se vea afectado todo el rendimiento de la red, limitando el daño al segmento respectivo.
- **Administración y gestión de red:** brinda facilidad de administración al manejar una estructura por capas, además de una fácil gestión de la red.

En el diseño se deben considerar tres parámetros: ancho de banda, redundancias y diámetro de la red. Se considera que debe existir un ancho de banda de mayor a menor desde el nivel de núcleo hasta el nivel de acceso. Las redundancias propuestas brindan disponibilidad a la red, por lo cual se debe duplicar las conexiones y el equipamiento activo. Se ha considerado las medidas del diámetro de la red en función de la mayor cantidad de equipamiento, la misma que es de tres.

a) Nivel de Núcleo

Este nivel es el backbone principal para la red de datos de la Institución y para los respectivos entes del MIDENA, este nivel manejará todo el tráfico proveniente de los equipos de la capa de distribución enviados hacia la red de datos, por lo cual el nivel de núcleo de la red debe contar con el equipamiento que le provea altas velocidades de transmisión.

Al manejar el backbone principal de comunicaciones de la red de datos es importante que los enlaces de conexión tanto hacia los diferentes entes de la red de datos como hacia su capa inferior sean a Gigabit permitiendo tener un mejor rendimiento en la red, además de aprovechar las características del equipamiento utilizado.

El equipamiento activo de este nivel cuenta con las siguientes características: puertos Gigabit Ethernet, manejo de puertos para estaqueo, funciones L2 y L3, manejo de VLAN[7], MSTP[8], STP[9] y agregado de enlace.

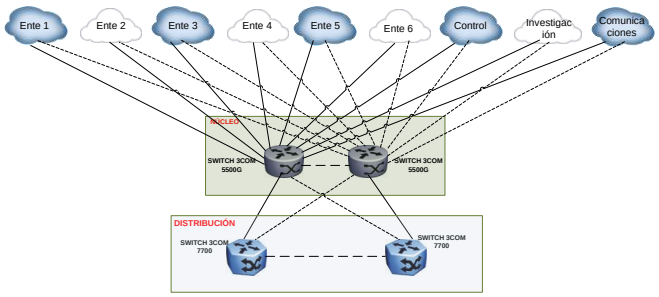

Fig. 2. Nivel de núcleo extendido del modelo de red

[4] ANSI: American National Standards Institute (Instituto Nacional Americano de Normalización)

[5] TIA: Telecommunications Industry Association (Asociación de Industrias de Telecomunicaciones)

[6] EIA: Electronic Industries Alliance (Alianza de Industrias Electrónicas)

[7] VLAN: Virtual Local Area Network (Redes de Área Local Virtuales)

[8] MSTP: Multiple Spannig Tree Protocol (Protocolo Múltiple de Spanning Tree)

[9] STP: Spanning Tree Protocol (Protocolo de Spanning Tree)

Dado que el diseño de red planteado es redundante es necesario utilizar MSTP (Protocolo Múltiple SpanningTree) para evitar tormentas de broadcast y un excesivo consumo de ancho de banda.

Debido a que el enrutamiento de tráfico utilizado para la red de datos es dinámico, como protocolo de enrutamiento se utilizará OSPF[10] manejando un área diferente en función de cada entidad.

b) Nivel de Distribución

Este nivel básicamente se encarga de todo el manejo de red interno de la institución y de entregar el tráfico generado desde la capa de acceso hacia el núcleo en el caso de la comunicación hacia la red de datos.

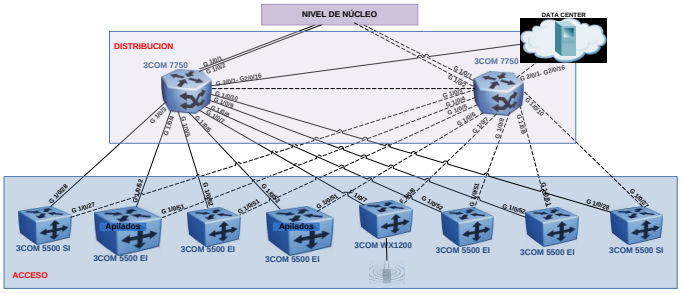

Fig. 3. Nivel de distribución del modelo de red

En la capa de distribución es importante que se maneje un tipo de equipamiento con buenas características de rendimiento además de que el mismo brinde disponibilidad y fiabilidad.

Entre las principales características del equipamiento de esta capa se tiene: switch modular de capa 3, soporte de L2 y L3, soporte de switching 10Gigabit, Gigabit y Fast Ethernet, soporte de PoE[11], soporte de ACL[12], MSTP, SNMP[13]v3, soporte de agregados de enlace y manejo de una plataforma de chasis.

El switch de esta capa manejará los enlaces de conexión con los bloques de la institución, además de los enlaces de conexión hacia los servidores de aplicación; además, el switch manejará todo el tráfico generado en la red interna y tendrá a cargo el manejo de inter VLANs de la red de la institución.

En este nivel se maneja un tipo de protocolo dinámico establecido como estándar OSPF, para publicación de las redes internas.

c) Nivel de acceso

Este nivel se encarga básicamente de brindar conectividad hacia el usuario final integrando todos los equipos de red finales como computadores, impresoras de red, teléfonos IP[14], cámaras IP, entre otros; además en este nivel se controlan los equipos que se conectan a la red.

[10] OSPF: Open Shortest Path First (Primero el Camino Libre más Corto)
[11] PoE: Power Over Ethernet (Poder sobre Ethernet)
[12] ACL: Access Control List (Listas de Control de Acceso)
[13] SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)
[14] IP: Internet Protocol (Protocolo de Internet)

Fig. 4. Nivel de acceso del modelo de red

En este nivel es importante que se manejen aspectos referentes a:

- **Facilidad de la conexión de los dispositivos de nodo final a la red:** a fin de que sea transparente para el usuario final y para las aplicaciones que se encuentran en este nivel.
- **Manejo de VLAN:** son un componente importante en redes convergentes, éstas permiten segmentar los dominios de broadcast, aumentar ancho de banda y brindar mayor seguridad. Los switches de la capa de acceso deben permitir establecer las VLAN para los dispositivos de nodo final en la red.
- **Velocidad de puerto:** se pueden considerar dos tipos de puertos Fast Ethernet y Gigabit Ethernet.
- **Agregado de enlaces:** permiten que el switch utilice múltiples enlaces simultáneamente agregando ancho de banda hasta los switches de capa distribución.
- **Listas de control de Acceso:** permiten controlar el tráfico cursante en la red.
- **Control de Acceso a la red:** utilizado para indicarle al switch los dispositivos que se pueden conectar a la red. Este tipo de seguridad de puerto se aplica en el nivel de acceso de manera que sea la primera línea de defensa para la red. La tecnología 3Com permite realizarla basada en:
  - Dirección MAC[15]
  - Dirección MAC y dirección IP.
- **PoE:** de ser necesario se puede considerar que los switches soporten Power Over Ethernet (PoE).
- **QoS:** la red se debe preparar para que sea convergente y admita tráfico de red de datos, voz y video, para lo cual los switch de capa de acceso necesitan admitir QoS para mantener la prioridad del tráfico. (Por ejemplo el tráfico de voz sobre el de datos).

Dentro del diseño se ha considerado la segmentación a nivel lógico de la red, la misma que permite a los usuarios además de la movilidad, seguridad, facilidad de escalabilidad.

Considerando los constantes cambios que se realizan en la infraestructura de red es necesario actualizar los diagramas de topología y documentación siempre que exista un cambio en la misma, teniendo en cuenta:

- Interconexión de los switches y el puerto del switch que interconecta los dispositivos.
- Rutas redundantes o los puertos agregados entre los switches que aportan rendimiento.

[15] MAC: Media Access Control (Control de Acceso al Medio)

- Identificación de las nuevas variantes de configuración en los switches.
- Actualización de la información acerca de las densidades de puertos de los dispositivos y de las comunidades de usuarios (grupos de usuarios).
- Cambio o asignación de puertos del equipamiento activo y usuarios finales.
- Puertos del equipamiento activo con control de acceso a la red.

2) Segmentación y direccionamiento IP

Dentro de los parámetros de diseño de la red de datos se considera la seguridad en el tráfico cursante entre cada una de las redes. Una segmentación a nivel lógico basada en VLAN además de brindar seguridad limita los dominios de broadcast presentes en la red, simplifica su administración y gestión al contar con una mejor organización de la red.

a) Segmentación y Direccionamiento IP para la Red de Datos

Cada uno de los entes pertenecientes al Ministerio de Defensa utilizarán una VLAN diferente de manera que se controle y proteja el tráfico cursante por su respectiva red.

b) Segmentación y Direccionamiento IP para el nivel de Acceso

Partiendo del levantamiento de red a nivel de usuarios, funciones y departamentos, uso de recursos y el Orgánico Funcional vigente de la institución, se segmenta la red en grupos o VLAN. Su agrupación está dada de manera independiente de su ubicación física.

En el diseño se propone la creación de 36 VLAN determinadas según los departamentos y necesidades de red, considerándose además un margen de crecimiento pensando en el incremento futuro de usuarios en la red para cada una de las VLAN.

La asignación del direccionamiento IP para cada una de las VLAN está basado en un direccionamiento eficiente VLSM[16], el cual permite la asignación utilizando una máscara variable optimizando el uso de la redes determinadas para la institución.

3) Listas de Control de Acceso

Las listas de control de acceso (ACL) permiten filtrar los paquetes de datos permitiendo o denegando el tráfico cursante, de manera que se limite el tráfico en la porción de red requerida.

Las listas de acceso creadas pueden ser aplicadas tanto para el tráfico de entrada "inbound" como para el tráfico de salida "outbound" dependiendo de la aplicación que se le desee dar.

Con el objeto de limitar el tráfico cursante en la red, en la institución se sugiere dos grupos de ACL diferentes:

- **Listas de acceso básicas:** utilizadas para limitar el tráfico generado por las diferentes redes.
- **Lista de acceso avanzada:** utilizadas para limitar la administración del equipamiento activo a la VLAN de Administradores.

Estas listas de control de acceso serán configuradas en los switch del nivel de acceso.

4) Propuesta de etiquetación.

Es importante tener en cuenta la identificación de los puntos de red de manera que se cuenta con una etiquetación que facilite la ubicación del punto de red, debiendo tener en cuenta los siguientes aspectos:

- **ID Bloque**: Permite una fácil identificación del bloque al cual se brinde el servicio de red.
- **Tipo de servicio (Tipo)**: Permite determinar el tipo de servicio prestado sea de voz o de datos.
- **Número de Patch Panel (#PP)**: Permite identificar el patch panel en el cual se encuentra conectado el punto de red.
- **Número del Punto de Red**: Permite identificar el número del punto de red según su ubicación en patch panel con su correspondiente salida a nivel de punto de red en las salidas de telecomunicaciones. Su identificación se la realizará utilizando los número del 01 al 48, para facilitar su lectura.

Ejemplo:

El punto de red de datos D-025 ubicado en el patch panel 1 del Bloque 1 se lo etiquetaría como:

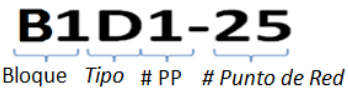

Fig. 5. Ejemplo de propuesta de etiquetación

Este modelo de etiquetación permite tener una idea clara de la ubicación del punto de red en cuestión, identificando claramente el bloque, el servicio prestado y su ubicación en patch panel.

IV. Simulación del Diseño de las Topologías de Red

Una vez desarrollado el diseño para la Red de Datos se hace necesario validar la operatividad del modelo propuesto. Teniendo en cuenta tanto los criterios técnicos como los requerimientos que presenta la Red de Datos de la Institución, se realizará la simulación aplicada al mismo.

A. TOPOLOGÍAS

El diseño de la topología desarrollado en la etapa de diseño basado en un modelo jerárquico permite identificar de manera clara la propuesta para la Red de Datos de la Institución.

La topología física muestra la distribución del equipamiento activo y los enlaces de conexión realizados entre el equipamiento de comunicaciones, en cambio la topología lógica muestra la segmentación basada en vlans, aplicada para cada una de las capas. Con la ayuda de las topologías mostradas se puede identificar la importancia y necesidad de las configuraciones realizadas.

[16] VLSM: Virtual Local Area Network (Redes de Área Local Virtuales)

1) *Topología Física*

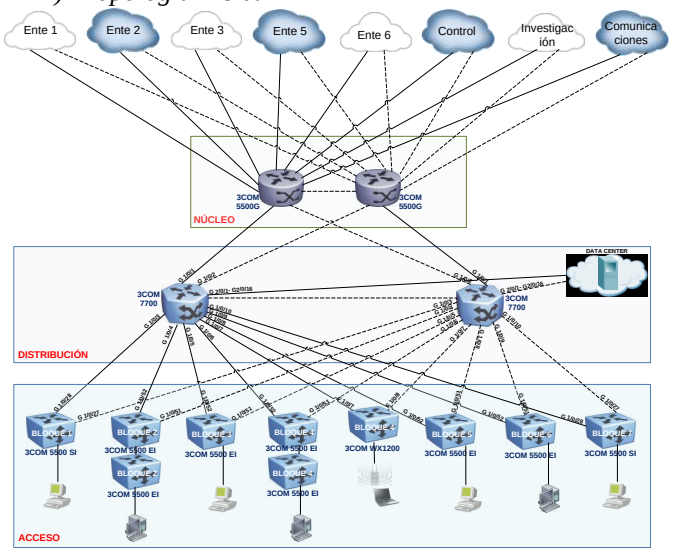

Fig. 6. Topología física de la red

2) *Topología Lógica*

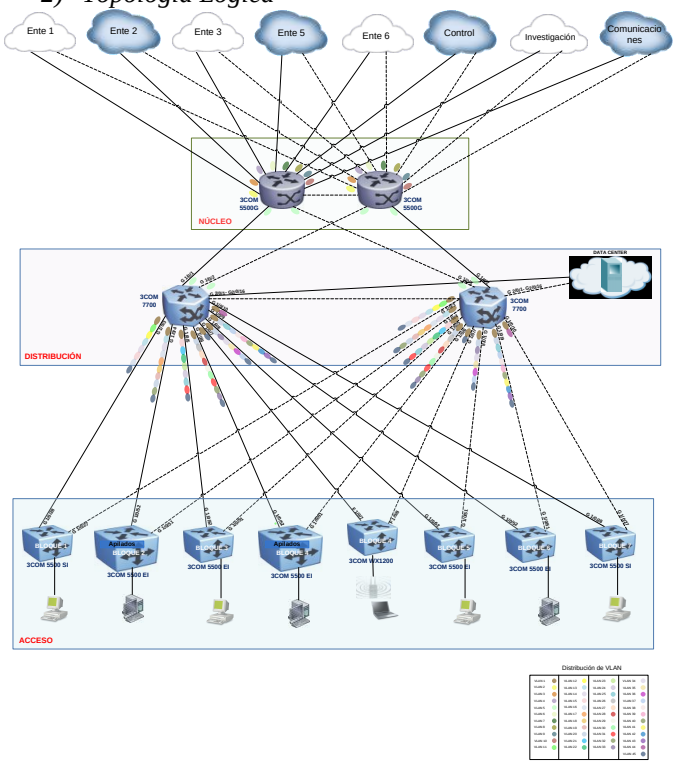

Fig. 7. Topología lógica de la red

La distribución de VLAN utilizada en la figura 7 se amplía en la siguiente figura:

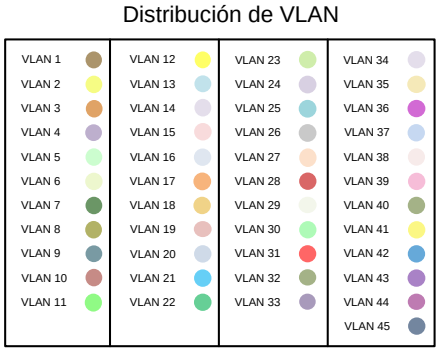

Fig. 8. Distribución de VLAN

B. *SIMULACIONES*

Para el desarrollo de las simulaciones que justifiquen el funcionamiento del diseño propuesto, se ha utilizado un simulador presente en el Mercado denominado Packet Tracer propietario de Cisco, dado que no existen simuladores para la tecnología 3Com que soporten las funcionalidades a demostrarse en el mismo.

Packet Tracer es una herramienta utilizada con objetivos educativos que permite realizar simulaciones de manera interactiva. La versión utilizada es 5.3.1, la misma que entre sus mejoras incluye switches capa 3 necesarios para la realización de las simulaciones.

Dentro de los equipos que ofrece el simulador cisco se tienen adicional a switches genéricos, los switches serie 2950, 2960 y 3560. Los switches 2950 y 2960 son equipos capa 2, brindan seguridad a nivel de puerto, manejan un número máximo de vlan de 255, puertos Fast Ethernet y Giga Ethernet, soporte de LACP[17] y ACL basadas en puertos. En cambio el switch 3560 es un switch capa 3, puertos Fast Ethernet y Giga Ethernet, soporta RSTP[18], PVRSTP, soporte de vlans, Soporte de PoE, LACP, Enrutamiento estático y Dinámico, Ruteo intervlan y manejo de ACL.

Dado que estos equipos brindan las características necesarias para la realización de la simulación del diseño propuesto los mismos serán utilizados en función del modelo diseñado.

Una síntesis de las características de los modelos de equipos Cisco se muestra a continuación:

Tabla 1. Características equipamiento Cisco [33]

Características	**Switch CISCO 2960**	**Switch CISCO 3560**
Seguridad a nivel de puerto	X	X
Puertos Gigabit Ethernet	2	2
Puertos Fast Ethernet	24	24
Soporte de RSTP		X

[17] LACP: Link Aggegation Control Protocol (Protocolo de Control de Agregación de Enlace)

[18] RSTP: Rapid Spanning Tree Protocol (Protocolo Rápido de Spanning Tree)

IEEE 802.1.Q	X	X
Capacidad de Capa 2	X	X
Capacidad de Capa 3		X
Soporte de PoE	X	X
Manejo de ACLs	X	X
Enrutamiento Estático		X
Enrutamiento Dinámico OSPF		X
Soporte SNMP	X	X
Stacking	X	X
Switch Modular	-	-
Soporte para Agregado de Enlaces	X	X
Fuentes de poder Redundantes	-	-

1) Topologías de Red

La topología que se muestra a continuación, muestra los criterios aplicados para brindar alta disponibilidad a la red, con la utilización de dos equipos robustos manejados a nivel de núcleo. Cada uno de los demás equipos simulan el equipamiento utilizado para cada uno de los entes de las demás intituciones adscritas al mismo.

Para cada uno de los diferentes entes se manejan dos enlaces, cada uno de ellos está conectado hacia uno de los switches de núcleo, en los cuales a su vez se utiliza el protocolo Spanning Tree para evitar que se produzcan lazos en la red. Con la topología mostrada se tiene un esquema HA dado que si un enlace falla automáticamente el enlace secundario tomará el control permitiendo que la red siga operativa.

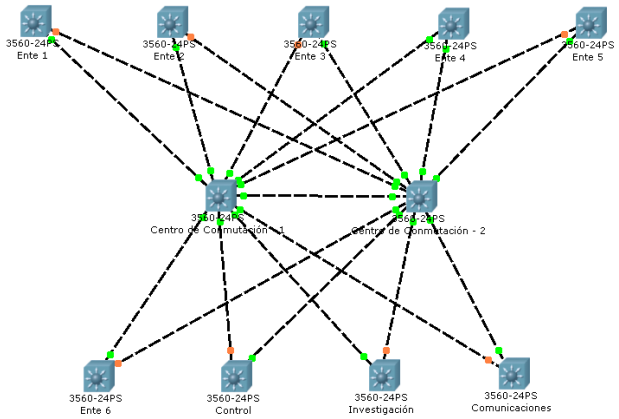

Fig. 9. Topología en Alta Disponibilidad

La figura 9 muestra la configuración de las diferentes vlan tanto a nivel de distribución como a nivel de núcleo de manera que se limita los dominios de broadcast en la red. Además en el mismo se han implementado políticas de seguridad para el control de acceso hacia el equipamiento activo.

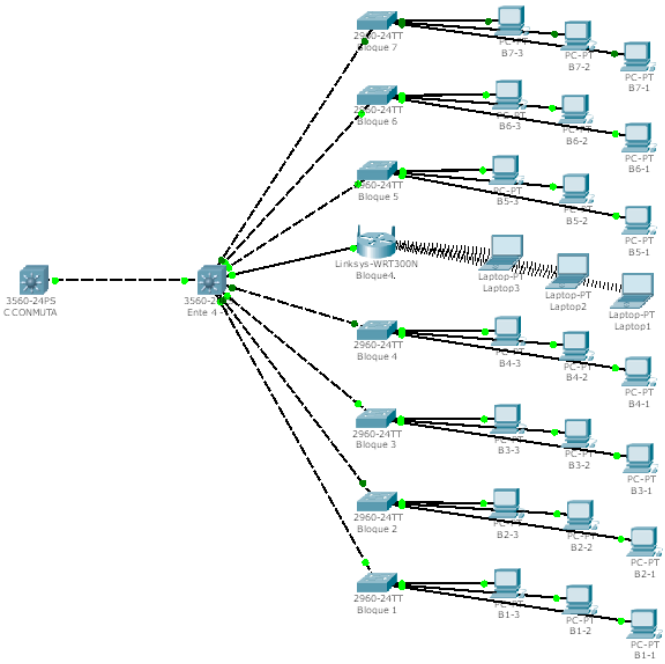

Fig. 10. Topología de la red de datos de la Institución

Para el desarrollo de las configuraciones se tomó como base los datasheet[19] del equipamiento.

C. OBJETIVOS FUNCIONALES

1) Seguridad

Uso de contraseñas para limitar el acceso local y remoto.- dado que mediante el acceso a la configuración del terminal se accede a las tareas de administración del equipamiento, es importante que se proteja el acceso mediante el uso de contraseñas de manera cifrada.

Uso de contraseñas cifradas y secretas.- en primera instancia las contraseñas para acceso local y remoto son guardadas en texto plano; el uso de contraseñas secretas y el servicio para encapsular las mismas, permite proteger las contraseñas dentro de los archivos de configuración del equipo. Además de esta manera se protegen las contraseñas ante la presencia de analizadores de tráfico.

Limitación de accesos por el terminal virtual.- es importante definir los usuarios que pueden acceder hacia la administración remota del equipo, de forma que solo personal autorizado (Administradores de red), pueda acceder a la misma. Con la aplicación de ACL de acceso se permite o niega sesiones establecidas.

Configuración de accesos SSH[20]:- como es conocido telnet no es protocolo seguro, por tal motivo es necesario establecer accesos tipo ssh de forma que se permita acceder de manera segura hacia el equipamiento de manera remota, de preferencia utilizando la versión 2.

Restricción de SNMP mediante el uso de ACL.- dado que para realizar el monitoreo de red hacia el equipamiento activo es necesario que se habilite SNMP en los equipos, es

[19] Tomados de la página oficial de Cisco http://www.cisco.com
[20] SSH: Secure Shell (Intérprete de Comandos Seguro)

importante que se definan las direcciones habilitadas para el acceso hacia los mismos.

Segmentación de red.- el aplicar microsegmentación a nivel de red permite que se manejen grupos con características y funciones similares, asegurando su conectividad y seguridad.

La aplicación de microsegmentación además prepara a la red para la aplicación de seguridad a nivel de equipos dedicados para ello.

2) Disponibilidad

Manejo de rutas redundantes.- Con la habilitación de rutas redundantes y la implementación de enlaces alternos se maneja una estructura en alta disponibilidad, de manera que se asegura la continuidad del servicio, en caso de que falle un enlace al detectarse en la topología un cambio de estado, se habilita el segundo enlace. La topología con enlaces redundantes permite brindar alta disponibilidad en la red y asegurar la prestación de los servicios de red.

Habilitación del protocolo Spanning Tree.- permite que se maneje una estructura en HA libre de lazos debido a que siempre se mantiene activo un canal mientras que el segundo se mantiene a la escucha.

3) Escalabilidad

Manejo de topología jerárquica.- La aplicación del modelo permite a la red agregar nuevos dispositivos sin que ello implique la disminución del rendimiento de la misma, el uso de un modelo jerárquico de red asegura su escalabilidad sin que se cause una degradación del servicio.

4) Desempeño

Eliminación de cascadas de red.- La utilización de apilamiento a nivel de equipos de red de la capa de acceso mejora el rendimiento de la red, al manejar como un único switch más grande, reduciendo además los dominios de broadcast generados en la misma, y facilitando su administración.

Limitación de dominios de broadcast.- el empleo de microsegmentación a nivel de red permite limitar los dominios de broadcast y mejorar el rendimiento en la misma.

Optimización del direccionamiento IP.- el aplicar un diseño adecuado de segmentación de red optimiza el uso de las redes asignadas hacia la institución.

Topología de red.- mediante el diseño de red se optimizó el uso de los recursos al ubicar el equipamiento en función de las características y necesidades de la red.

5) Flexibilidad

Manejo de topología jerárquica.- El diseño de un modelo aplicando una topología jerárquica permite realizar cambios, modificaciones o adiciones de equipamiento de red de manera que se adapte al crecimiento de las misma.

A nivel de una topología jerárquica el agregar equipamiento se facilita, debido a que cada una de sus capas puede crecer sin ninguna dificultad técnica y sin afectar el rendimiento de la red.

Microsegmentación de red.- permite que la red se adapte a los cambios que se produzcan en la misma independientemente de la ubicación física a la cual se asignen a los usuarios en la institución, asegurando la conectividad con los usuarios del mismo segmento de red.

V. Conclusiones

- El desarrollo del presente proyecto permitió ofrecer a la institución, un modelo que optimiza el uso de la red de datos, por medio de la aplicación de la topología de red basada en una estructura jerárquica brindando características de alta disponibilidad, escalabilidad, flexibilidad además de seguridad para la misma. Además, la estructura de red permite el fácil aislamiento de segmentos en caso de presentarse problemas en alguno de ellos o por motivos de mantenimiento, permitiendo que el resto de la red continúe operando.
- Teniendo en cuenta la importancia de los servicios brindados por medio de la red de datos, el manejo de una infraestructura redundante a nivel tanto de equipamiento como de enlaces asegura la disponibilidad de los servicios, permitiendo contar con una red completamente operativa.
- El estudio de la infraestructura de la red permite conocer a detalle las fortalezas y falencias de la red, con lo que se ha desarrollado un modelo que se adapte a sus requerimientos y exigencias, estableciéndose un modelo funcional para la red.
- La validación de las normas y estándares de cableado estructurado, además de la certificación de los puntos de red, permite asegurar tanto la conexión hacia la red como el acceso hacia el canal de comunicaciones.
- La aplicación de microsegmentación a nivel de red reduce el alcance de los dominios de broadcast al segmentar la red en pequeños grupos que comparten características similares, permitiendo el acceso a determinadas vlan o usuarios y restringiendo el resto, de manera que se brinde mayor seguridad a la red.
- La aplicación de listas de control de acceso tanto asociadas a la administración del equipamiento activo como para la restricción del tráfico cursado entre las diferentes vlan asignan seguridad a la red y permiten mejorar el rendimiento de la misma.
- La habilitación de protocolos seguros para la administración del equipo brinda mayor seguridad a la red protegiéndola ante ataques mal intencionados.
- El desarrollo de las configuraciones en equipamiento de tecnología 3Com y la simulación del modelo propuesto en un simulador del mercado permite evidenciar que de manera independiente de la infraestructura del equipamiento que se maneje, el modelo es enteramente funcional. Debiendo tenerse en cuenta que ciertas características varían en

relación a la tecnología de equipamiento utilizado, sin embargo el modelo cumple con todos los objetivos funcionales dado que los criterios aplicados son los mismos

REFERENCIAS

[1] Castells,Manuel,(2010). The rise of the network society. Chichester, West Sussex ; Malden, MA : Wiley-Blackwell
[2] Lazaro Laporta, Jorge, (2002). Fundamentos de telemática. Editorial de la UPV. Valencia
[3] Tanenbaum, Andrew, (2003). Redes de computadoras. 4ed.Mexico, D. F. Pearson Educacion
[4] Paquet, Catherine y Teare, Diane, (2001). Creación de redes cisco escalables. Pearson Educacion, S.A., Madrid
[5] SHELDON Tom, LAN TIMES: Enciclopedia de redes networking, Mc Graw-hill, México, 1994.
[6] PARNELL Tere, LAN TIMES: Guía de redes de alta velocidad, Mc Graw-hill, Madrid, 1997.
[7] JENKINS Neil, Redes de área local, Prentice Hall, México, 1996.
[8] FORD Merilee, Tecnologías de interconectividad de redes, Prentice Hall, México, 1998.
[9] 3Com, 3COM Stackable switch family-advanced configuration guide, 3Com Corporation.
[10] Cisco Systems, Academia de networking de cisco systems guía del segundo año CCNA 3 Y 4, Pearson Educación, Madrid, 2004.
[11] Stallings, Williams (2000). Comunicaciones y redes de computadores. Madrid/ Prentice- Hall/ c2000
[12] McQuerry, Steve, (2004).Interconexión de dispositivos de red cisco libro de autoestudio CCNA 2ed. Pearson Educacion, S.A., Madid, 2004
[13] TIA/EIA STANDARD, (2001). Commercial Building Telecommunications Cabling Standard. TIA/EIA-568-B. Telecommunications Industry Association.
[14] TIA/EIA STANDARD, (2004). Commercial Building Standard for Telecommunications Pathways and Spaces. TIA/EIA-569-B. Telecommunications Industry Association.
[15] TIA/EIA STANDARD, (2002). Administration Standard for Commercial Telecommunications Infraestructure. TIA/EIA-606-A. Telecommunications Industry Association.
[16] TIA/EIA STANDARD, (2002). Commercial Building Grounding (Earthing) and Bonding Requirements For Telecommunications. J-STD-607-A. Telecommunications Industry Association.
[17] http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml
[18]http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf----vlan
[19] http://www.unsa.edu.pe/infounsa/cursor/01/cursor01.pdf
[20] http://es.kioskea.net/contents/internet/vlan.php3
[21]http://www.commserv.ucsb.edu/infrastructure/standards/history/EIA-TIA_568.asp
[22] http://www.dte.us.es/personal/mcromero/docs/arc1/tema2-arc1.pdf
[23] http://www.ansi.org/
[24]http://www.rfc-es.org/rfc/rfc1918-es.txt
[25] http://www.ecaus.org/eia/site/index.html
[26] http://www.alfinal.com/Temas/cableadoestructurado.php
[27]http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/CableadoEstructurado2.pdf
[28]http://www.tiaonline.org/standards/
[29] http://www.luguer.com/catalogos/pdf/DTX_ES.pdf
[30] http://www.flukenetworks.com/datacom-cabling/copper-testing/LinkWare-Stats
[31] http://h17007.www1.hp.com/us/en/index.aspx
[32] http://www.fingertec.com/images/w_brochure/AC900_e.html
[33] http://www.cisco.com

BIOGRAFIAS

Ramón I. Nancy Y. Nació en Ibarra provincia de Imbabura, el 26 de agosto de 1986. Realizó sus estudios primarios en la Escuela Ana Luisa Leoro, obtuvo su bachillerato en el Colegio Nacional Ibarra. Ingreso a la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte en el año 2004, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación. Realizó sus prácticas preprofesionales en la empresa Invetrónica Cía. Ltda en el departamento técnico, realizando tareas de Diseño de Antenas, Estudios de Ingeniería, Programación de Equipos de Radiocomunicación y Reparación de Fuentes de Alimentación; en la Universidad Técnica del Norte – Edif. Biblioteca realizó tareas de Análisis, Valoración, Certificación y Rectificación de puertos de red ; en la empresa RedSoluciones se desempeñó en el Área de Redes, desarrollando tareas de Análisis y Diseño de Redes, Configuración de equipos L2 y L3, Levantamiento de Información de Red, Configuración, Administración y Capacitación en Herramientas de Monitoreo e Inventario IP y Monitoreo y Gestión de Red.

Carlos A. Vásquez A. Nació en Quito provincia de Pichincha el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones (CUM LAUDE), Escuela Politécnica Nacional (EPN) en Quito-Ecuador en 2008. Actualmente es Docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, dictando las materias de Networking II y III, Proyectos de Redes, Administración de Redes. Cumple la función de vocal principal del Consejo Académico de la Carrera de Ingeniería en Electrónica y Redes de Comunicación. Aprobó los cursos CCNA 1, 2 ,3 ,4 de estudiante en el período junio 2006 – marzo 2007 en la Escuela Politécnica Nacional y el CCNA 1 de Instructor en la ESPOL, y cursa la Maestría en Redes de Comunicación (2do Semestre), Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Reengineering of Data Network of an Entity of the Ministry of National Defense (MIDENA)(March 2012)

Nancy Yolanda Ramón Ibujés

Director: Ing. Carlos Vásquez

***Abstract* — This paper proposes a design which improves the network performance, proposing a scheme based on a detailed study of its infrastructure and current requirements, by applying a hierarchical model based on the study of layers and microsegmentation logical level of the network, as well as the implementation of a scheme that ensures continuity of service. With the development of the simulation demonstrates the functionality of previously established model using Packet Tracer 5.3.1 software which provides an interface that facilitates validate settings made, showing its operation in regardless of the technology infrastructure used.**

The development of this project provides an efficient solution for the Data Network of the Institution under which enhances performance and the service provided both to the different entities associated as to the internal network, considering the current infrastructure which it has.

I. INTRODUCTION

The Ministry of Defense is the political and administrative executive, responsible for directing the Defense Policy and managing Armed Forces to harmonize their actions between state functions and the Military Institution.

Within the national framework, the Armed Forces must combine their actions with the Social National and International Development, and contrast with the advancement of science and technology that allows meeting new challenges, risks and threats in Pro National Interests.

In this context the Entity of the Ministry of National Defense under consideration is one of the planning agencies and military leadership whose internal structure should allow a quick action before making important decisions for the benefit of all inhabitants of the nation, protecting its sovereignty.

Due to the nature of services, it is necessary that the network has high availability and quality of service through a network infrastructure that supports large amounts of traffic, besides having scalability and flexibility.

For the development of network design that meets the above factors, it is necessary to develop various preliminary stages, with which at first known the current network situation and then proceed to develop a design that fits your needs and meet your requirements.

II. ANALYSIS OF THE STATE DATA NETWORK

In order to determine the current status of the data network is made a situational study, which shows the requirements relating to services and network security.

The development of the network lifting involves key aspects such as structured cabling, physical and logical structure of the network, users and their role within each department, location and status of network points, behavior of the electromagnetic spectrum within the facility, addition to the elements that make up the active part of the network, i.e. the study should reflect in detail their situational state.

Structured Cabling is the essential foundation for the provision of network services, so it is important that it is in perfect condition.

Within the collection of information of the structured cabling should consider the following elements: horizontal cabling, vertical cabling, work area, telecommunications room and equipment room, entrance facilities and grounding system. In addition to the lifting of each of the elements described, must identify the rules and structured cabling standards, which can ensure the connection first and then the network communication.

Depending on the age of cable systems is worthwhile to make a certification of structured cabling, so as to determine its status and performance, the certification of network points determine compliance or noncompliance of the network parameters and in turn validates compliance with structured cabling rules and standards based on the TSB[21] 67. Based on the certification report can define the operation of the structured cabling system or give the justification for the change of it, since it does not provide the features that ensure

[21] TSB: Technical Service Bulletin

communication in relation to the demand for the services offered by the institution

Physical and logical structure.- The rise of the network infrastructure also involves locating all active elements of the network; determine its connection model, in addition to setting up each of the equipment, so as to identify the topology managed at the logical level in the network infrastructure of the institution.

The diagram of the network topology can clearly identify the status of the network from an operational perspective, it is important that your analysis is divided into at least two parts: an external perspective view or the Internet and another from an internal perspective or intranet with its constituents. The internal view may be subdivided according to the networks that are managed inside so that you can point out your survey, identifying the network equipment, connections between them and especially the security issues associated. With the logical topology is identified network segmentation used, potential bottlenecks in the network, broadcast domains, critical paths, among others.

With the analysis of network equipment configurations can also determine the security problems in your setup, mainly associated with the use of passwords, access protocols unsafe and unnecessary settings.

Throughout the network infrastructure is important to keep updated these topologies, since they allow identifying graphically the network structure so that there is a tool for easy observation and analysis for quick action in making decisions.

Electromagnetic spectrum.- The study of the electromagnetic spectrum to identify the spectrum use allowing busy channels and determine the availability or saturation, as well as standards compliance. It is important that before introducing new channels in operation for a study to indicate their availability so as to avoid overlapping of signals due to abuse them, it is also important to have an optimal operating environment, respect channel spacing set to the IEEE 802.11 b, g**.**

Survey at end user level.- Identification of users on the network along with its location, function and requirements, allows us to detail the constituent elements in a network and its needs. It is important to consider the shared resources on the network, determining parameters for the establishment of a working model so as not affected the activities of users.

As network topologies, the rising level of end user along with its components, must be constantly updated and clearly identified, this document will be used by the administrator as a supporting document, which also facilitates the identification of faults.

The success of a network design depends on the stage of lifting of information within which the information is obtained which serves as basis for the development of the following stages. However during the data analysis is determined the requirements and needs to be taken into account in the design of the network, and the criteria to be considered for its design, so the design is functional for the network of the institution.

III. DESIGN OF PHYSICS AND LOGIC TOPOLOGIES

Within the design of network topologies are specified the most important parameters to be considered for the implementation of the model. However before starting the design approach is important to consider three aspects as: the growth forecast at the level of network users, policies implemented and the analysis of user requirements.

Given the estimated growth projection of the network, its design must meet the requirements with a fully operational infrastructure in terms of growth, taking into account also the demand for equipment that this implies. Instead predefined network policies at the institution provide the main guidelines of security and regulation of the use of facilities, equipment and services to be observed. For the design made to be functional also be taken into account the user requirements obtained during the collection of information, such as addition need of network points, resource sharing use, among others.

A. Reengineering the data network

After performed the analysis of information relating to network situational study of the institution and knowing its internal structure, there is the redesign of the data network, based on logical and physical structure studied, which provides a scalable network, flexible, easily managed, as well as available, to reduce the size of the existing broadcast domains, allowing a comprehensive solution for data network.

The design should help to improve the performance of the network to make best use of existing equipment with proper management, making drastic changes on it.

The network re-engineering takes into account the level design analysis of structured cabling, it is based on compliance with ANSI[22]/TIA[23]/EIA[24]-568-B, ANSI/TIA/EIA-569, ANSI/TIA/EIA-606-A and ANSI/TIA/EIA-J-STD-607-A.

1) Network Model

The redesign solution to the data network of the institution should provide the network to be easily managed with ease of expansion, available, secure and able to solve problems quickly, these features are provided by a network model of hierarchical.

The above model is based on the design and structure of layers within which each has its specific function and role in the network, thus differentiate three layers:

- Core
- Distribution and
- Access.

[22] ANSI: American National Standards Institute
[23] TIA: Telecommunications Industry Association
[24] EIA: Electronic Industries Alliance

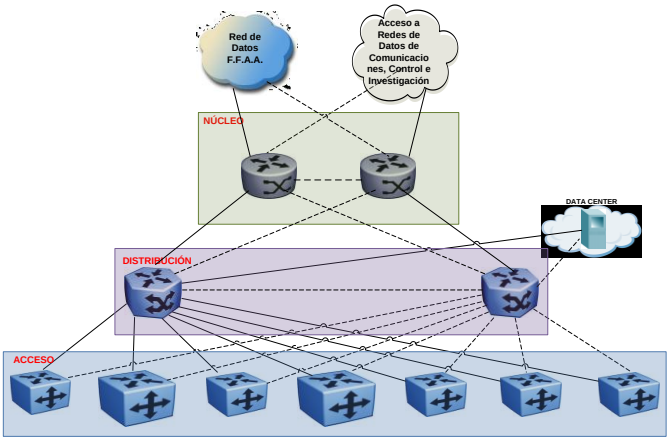

Fig. 11. Network General Model

The figure shows in a general way the network model proposed for the institution, according to which for each of the layers is defined functionality, equipment and characteristics of each.

Among the advantages of the model include:

- **Scalability:** easy growth and expansion, its growth is from the level of access to the core level, depending on need and availability of ports.
- **Performance:** the core and distribution switches to have good handling characteristics at high speeds, avoiding having bottlenecks in the network.
- **Security:** policies are allowed to manage both the distribution level switches as in the access level allowing set policies to port level.
- **Redundancy:** high availability allows the network to avoid having service falls.
- **Fault isolation:** isolate defective equipment so as not to be affected all the network performance by limiting the damage to the respective segment.
- **Network Management:** provides ease of administration to manage a layer structure, as well as easy network management.

The design must consider three parameters: bandwidth, redundancy and network diameter. It is considered that there must be a bandwidth of high to low level from the core to the access level. Proposed redundancies provide to the network availability, so you must duplicate the connections and the active equipment. It has been considered the diameter of the network based on the largest amount of equipment, the same that is three.

a) Core Level

This level is the main backbone data network of the institution and for the respective entities of MIDENA , this level will handle all the traffic from equipment on the distribution layer sent to the data network, so the level of core of the network must have the equipment that will provide high-speed transmission.

When handling the main communications backbone of the data network is important for links both to the different entities of the data network and to your bottom layer are to Gigabit allowing a better network performance, as well as take advantage of characteristics of the equipment used.

The active equipment at this level has the following features: Gigabit Ethernet ports, stacking ports management, L2 and L3 functions, VLANs[25], MSTP[26], STP[27] management, and link aggregation.

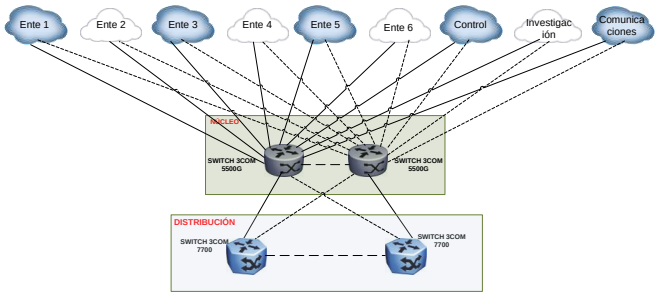

Fig. 12. Extended core level of the network model

Since the proposed network design is redundant need to use MSTP (Multiple Spannig Tree Protocol) to prevent broadcast storms and excessive consumption of bandwidth.

Because the routing of traffic used for the data network is dynamic, as the routing protocol is used OSPF[28] driving a different area based on each entity.

b) Distribution Level

This level basically does all the management of the institution's internal network and delivers the traffic generated from the access layer to the core in the case of communication to the data network.

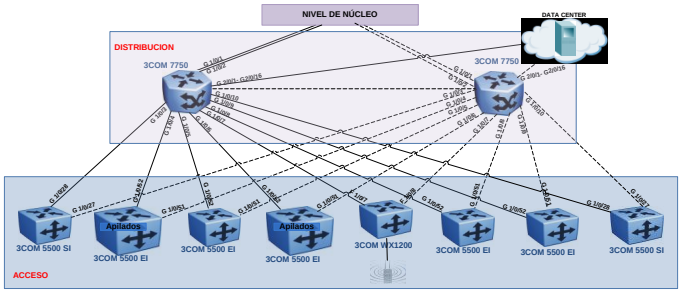

Fig. 13. Distribution level of the network model

In the distribution layer is important for handling a type of equipment with good performance characteristics in addition to that it provides availability and reliability.

[25] VLAN: Virtual Local Area Network
[26] MSTP: Multiple Spannig Tree Protocol
[27] STP: Spanning Tree Protocol
[28] OSPF: Open Shortest Path First

Key features of the equipment of this layer is: Layer 3 modular switch, L2 and L3 support, switching support 10Gigabit, Gigabit and Fast Ethernet, PoE[29] support, support for ACL[30], MSTP, SNMP[31]v3, support link aggregation and managing a chassis platform.

The switch of this layer will handle the links connecting the blocks of the institution, as well as the links connecting to application servers, in addition, the switch will handle all the traffic generated on the internal network and will be responsible for managing inter VLANs in the network of the institution.

This level manages a dynamic protocol type set to OSPF standard for publishing internal networks.

c) Access Level

This level is basically responsible for providing connectivity to end users by integrating all end network equipment such as computers, network printers, IP[32] phones, IP cameras, among others, at this level also control the computers that connect to the network.

Fig. 14. Access level of the network model

At this level it is important to manage issues relating to:

- **Ease of connecting end node devices to the network:** to be transparent to end users and applications that are in this level.
- **VLAN Management:** they are an important component in converged networks, they allow segmenting broadcast domains, increasing bandwidth and added security. Switches in the access layer should allow set the VLAN for end node devices on the network.
- **Port Speed:** you can consider two types of ports, Fast Ethernet and Gigabit Ethernet.
- **Link Aggregation:** allows the switch to use multiple links simultaneously adding bandwidth to the distribution layer switches.
- **Access Control Lists:** allow control traffic on the network.
- **Access Control to the network:** used to indicate to switch devices can be connected to the network. This type of port security is applied at the level of access so that it is the first line of defense for the network. 3Com technology lets do it based on:
  - MAC[33] address
  - MAC address and IP address.
- **PoE:** if necessary we can consider that the switches support Power Over Ethernet (PoE).
- **QoS:** the network must be prepared to be convergent and supports data network traffic, voice and video, for which the access layer switches, need to support QoS to maintain traffic prioritization. (E.g. voice traffic over data traffic).

Within the design has been considered the segmentation at logical level of the network that allows users to mobility, security, ease of scalability.

Considering the constant changes taking place in the network infrastructure is necessary to update the topology diagrams and documentation provided that a change in it, taking into account:

- Interconnection of switches and the switch port that connects the devices.
- Redundant paths or aggregated ports between switches that provide performance.
- Identification of new variants of switches configuration.
- Update the information about port densities of the devices and user communities (user groups).
- Changing or assigning active equipment ports and end users.
- Active equipment ports to control network access.

2) Segmentation and IP Addressing

Within the design parameters of the data network is considered the trainee traffic safety between each of the networks. A logic level segmentation based VLANs provide security in addition to limiting the broadcast domains in the network, simplifying administration and management to have a better organization of the network.

a) Segmentation and IP Addressing for Data Network

Each of the entities belonging to the Ministry of Defense will use a different VLAN so as to control and protect the trainee traffic by the respective network.

b) Segmentation and IP addressing for the level of access

From the Survey network of users' level, functions and departments, use of resources and Organic Functional existing at the institution, the network is segmented into

[29] PoE: Power Over Ethernet (Poder sobre Ethernet)
[30] ACL: Access Control List (Listas de Control de Acceso)
[31] SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)
[32] IP: Internet Protocol (Protocolo de Internet)
[33] MAC: Media Access Control (Control de Acceso al Medio)

groups or VLAN. His group is given independently of their physical location.

The design proposes the creation of 36 VLANs appropriated to departments and networking needs, considering also a margin for growth considering the future increase of users on the network for each VLAN.

The allocation of IP addressing for each VLAN addressing is based on an efficient VLSM, which allows assignment using a variable mask optimizing the use of certain networks for the institution.

3) *Access Control Lists*

The access control lists (ACLs) to filter the data packets allowing or denying trainee traffic, so as to limit the traffic on the network portion required.

Created access lists can be applied both inbound traffic outgoing traffic depending on the application that you want to.

In order to limit trainee traffic on the network, suggests two different ACL groups at the institution:

- **Basic access lists:** used to limit the traffic generated by the different networks.
- **Advanced Access list:** used to limit the administration of active equipment to VLAN Administrators.

These access control lists are configured on the switch on the access level.

4) *Proposal for labeling*

It is important to note identifying the network points so as to have a labeling to facilitate network point location, and must take into account the following aspects:

- **ID Block:** Allows an easy identification of the block to which they provide the network service.
- **Service type (Type):** Determines the type of service is voice or data.
- **Number of Patch Panel (# PP):** It identifies the patch panel which is connected to the network point.

Network Point Number: Allows you to identify the network point number according to their location in the patch panel with its corresponding output to network point level in the telecommunications outlets. Their identification was made using the number from 01 to 48, for readability.

Example:

The data network point D-025 located in the patch panel 1 of Block 1 would label it as:

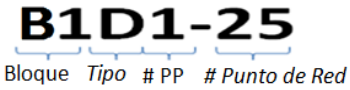

Fig. 15. Labeling proposal sample

This labeling model allows a clear idea of the location of network point in question, clearly identifying the block, the service provided and its location in patch panel.

IV. Network Topologies Design Simulation

Once developed the design for the data network is necessary to validate the operation of the proposed model. Taking into account the technical criteria and the requirements posed by Data Network of the Institution, will take effect at the same simulation.

A. *TOPOLOGÍAS*

The topology design developed in the design stage based on a hierarchical model clearly identifies the proposal for the Data Network of the Institution.

The physical topology shows the distribution of active equipment and feeder links made between the communications equipment, however the logical topology shows the segmentation based on VLANS, applied to each of the layers. With the help of the topologies shown you can identify the importance and necessity of your settings.

1) *Physical Topology*

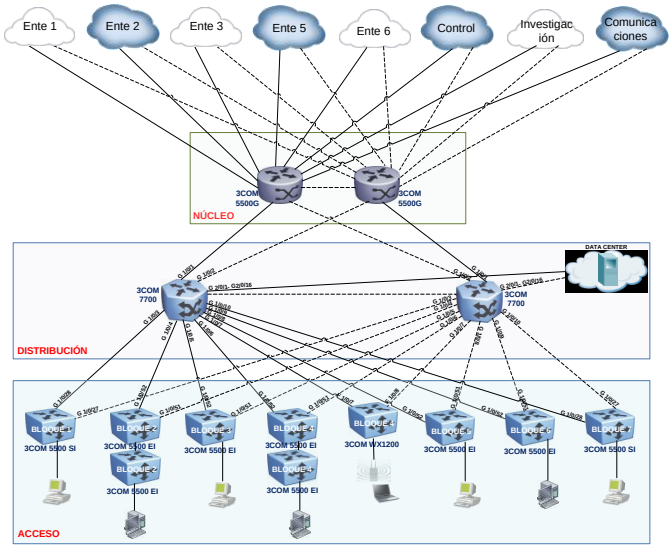

Fig. 16. Physical topology of the network

2) Logical Topology

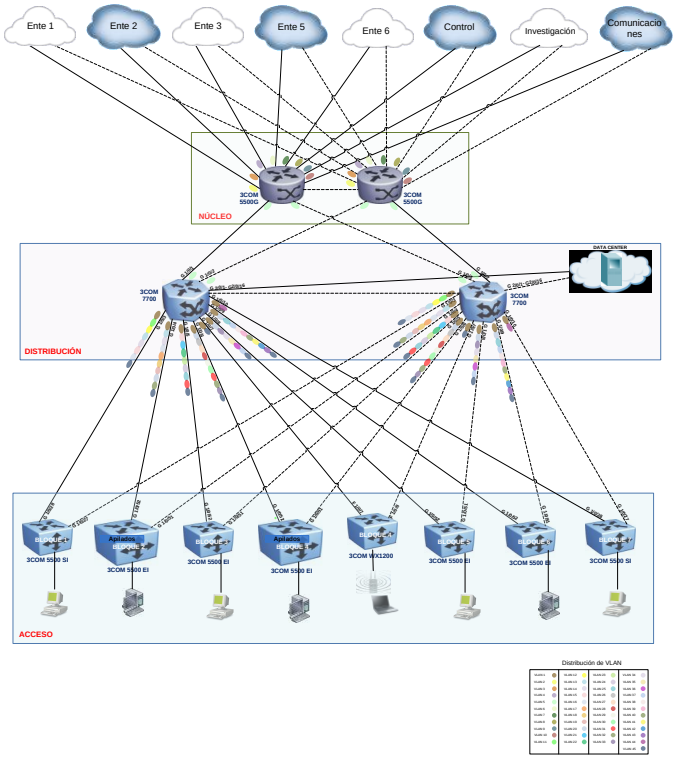

Fig. 17. Logical topology of the network

The distribution of VLAN used in Figure 7 is expanded in the following figure:

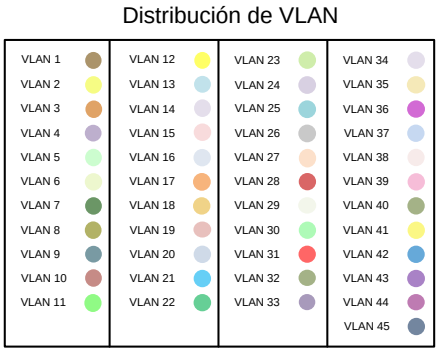

Fig. 18. Distribution of VLAN

B. SIMULATIONS

For the development of simulations to justify the operation of the proposed design, we used a simulator on the market called Packet Tracer, Cisco proprietary, since there are no simulators for 3Com technology that supports the functionality to be demonstrated in it.

Packet Tracer is a tool used for educational purposes that enables interactive simulations. The version used is 5.3.1, between their improvements include Layer 3 switches needed to perform the simulations.

Among the features offered by the simulator Cisco switches you have additional generic switches, series 2950, 2960 and 3560. 2950 and 2960 switches are Layer 2 devices, provide security at the port, handling a maximum number of VLAN 255, Fast Ethernet and Giga Ethernet, LACP support and port-based ACL. Instead, the switch 3560 is a Layer 3 switch, Fast Ethernet and Giga Ethernet, RSTP supports, PVRSTP, VLANs support, PoE support, LACP, static and dynamic routing, inter VLAN routing and ACL management.

Since these devices provide the features necessary for carrying out the simulation of the proposed design will be used in function of the model designed.

A summary of the characteristics of Cisco device models is shown below:

Tabla 2. Cisco equipment characteristics [33]

Features	**Switch CISCO 2960**	**Switch CISCO 3560**
Port level security	X	X
Gigabit Ethernet Ports	2	2
Fast Ethernet Ports	24	24
RSTP Support		X
IEEE 802.1.Q	X	X
Layer 2 Capacity	X	X
Layer 3 Capacity		X
PoE Support	X	X
ACLs Handling	X	X
Static Routing		X
Dynamic Routing OSPF		X
SNMP Support	X	X
Stacking	X	X
Modular Switch	-	-
Support for link aggregation	X	X
Redundant power supplies	-	-

1) Network Topologies

The topology below shows the criteria used to provide high availability to the network, using two robust teams managed to core level. Each of the other computers simulates the equipment used for each of the bodies of other equipment attached thereto.

For each of the different entities are handled two links, each connected to one of the core switches, in which in turn uses the Spanning Tree Protocol to avoid loops in the network. With the topology shown have a HA scheme because if one link fails the secondary link automatically takes control allowing the network to continue operating.

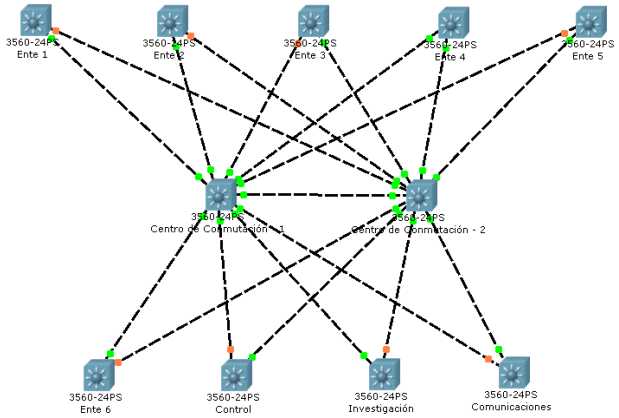

Fig. 19. High Availability Topology

Figure 9 shows the configuration of the different VLAN both at the distribution level to the core so that limited broadcast domains in the network. Also in those has implemented security policies to control access to the active equipment.

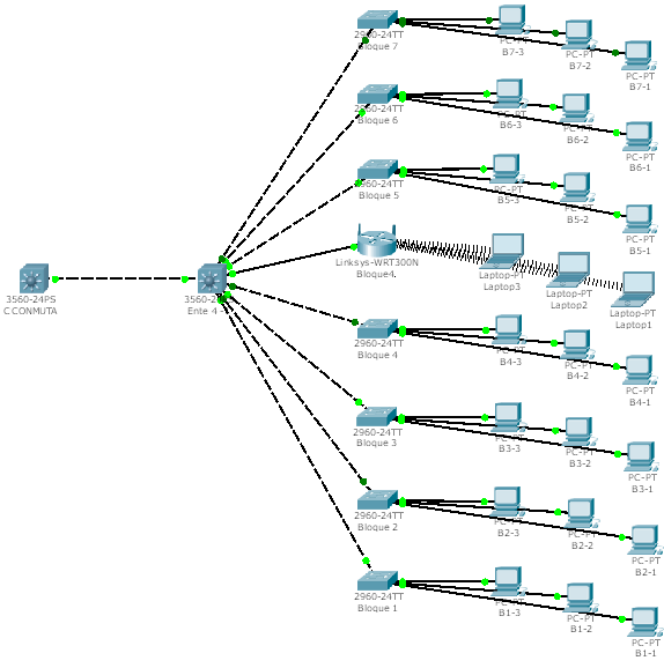

Fig. 20. Network data topology of the Institution

For the development of the configurations has been taken as a basis the equipment datasheet[34].

C. FUNCTIONAL OBJECTIVES

1) Security

Using passwords to limit local and remote access.- Since, by accessing the terminal configuration provides access to the equipment management tasks, it is important to protect access by using passwords in encrypted form.

Using encrypted and secret passwords.- In the first instance passwords for local and remote access are stored in plain text, use of secret passwords and service to encapsulate them, helps protect passwords in configuration files on equipment. Moreover in this way protects the passwords in the presence of traffic analyzers.

Access limitation by the virtual terminal.- Is important to define which users can access to the remote management of equipment, so that only authorized personnel (network administrators) can access it. By applying ACL allows or denies access sessions established.

Configuring SSH[35] access.- as known telnet is not secure protocol, for that reason you need to set type SSH access so as to allow secure access to remote equipment, preferably using version 2.

Restricting SNMP using ACL.- As for monitoring network to the active equipment is necessary to enable SNMP on equipments, it is important to define the addresses authorized to access to them.

Network segmentation.- Microsegmentation applying network level allows groups to be handled with similar features and functions, ensuring connectivity and security.

The application of microsegmentation also prepares the network for application-level security teams dedicated to it.

2) Availability

Management of redundant paths.- By enabling redundant paths and implementation of alternate links to manage a high availability framework, so as to ensure continuity of service, if a link fails to detect a change in the topology state, the second link is enabled. The topology with redundant links can provide high network availability and ensure the provision of network services.

Enabling Spanning Tree protocol.- Allows you to manage a structure in HA free bonds because always is provided an active channel while the second keeps the listener.

3) Scalability

Hierarchical topology management.- The application of the model allows the network to add new devices without incurring performance degradation, using a hierarchical model ensures network scalability without causing a degradation of service.

[34] http://www.cisco.com

[35] SSH: Secure Shell (Intérprete de Comandos Seguro)

4) Performance

Removing network cascades.- The use of stacking equipment at the network access layer improves the performance of the network, as a single switch handle larger, further reducing the broadcast domains generated therein, and facilitating administration.

Limiting broadcast domains.- The use of network level microsegmentation to limit the broadcast domains and improve performance in it.

Optimization of IP addressing.- Applying proper design of network segmentation optimizes the use of nets assigned to the institution.

Network topology.- By the network design was optimized using resources to locate equipment based on the characteristics and needs of the network.

5) Flexibility

Hierarchical topology management.- The design of a model using a hierarchical topology to make changes, modifications or additions network equipment so as to adapt to the growth of the same.

At the level of a hierarchical topology adding equipment is provided, because each of the layers can grow without any technical difficulty and without affecting the performance of the network.

Microsegmentation network.- Allows the network to adapt to changes occurring in the same regardless of physical location to which users are assigned to the institution, ensuring connectivity to users on the same network segment..

V. CONCLUSIONS

- The development of this project enabled the institution to offer a model that optimizes the use of the data network through the implementation of the network topology based on a hierarchical structure to provide high availability features, scalability, flexibility and safety. Furthermore, the network structure allows easy isolation of segments in case of disruption in one of them or for maintenance reasons, allowing the rest of the network continues to operate.
- Given the importance of the services provided through the data network, managing redundant infrastructure equipment at both links and ensures the availability of services, allows having a fully operational network.
- The study of network infrastructure allows knowing in detail the strengths and weaknesses of the network, which has developed a model that suits your requirements and demands, establishing a functional model for the network.
- Validation of norms and standards for structured cabling, in addition to the certification of network points, ensures both the connection to the network as access to the communications channel.
- The application of network-level microsegmentation reduces the scope of broadcast domains by segmenting the network into smaller groups that share similar characteristics, allowing access to specific users and restricting VLAN or the other, so as to provide greater security network.
- The implementation of access control lists associated with both the administration of active equipment to the restriction of traffic carried between different VLAN assigned to the network security and to improve the performance of it.
- Enabling secure protocols for the management equipment provides greater security for protecting the network against malicious attacks.
- The development of the settings in 3Com technology equipment and simulation of the proposed model in a market simulator allows to show that independently of the infrastructure of equipment is handled, the model is fully functional. Must be noted that certain characteristics vary in relation to the technology of equipment used, however the model meets all functional objectives since the criteria applied are the same.

REFERENCES

[1] Castells,Manuel,(2010). The rise of the network society. Chichester, West Sussex ; Malden, MA : Wiley-Blackwell

[2] Lazaro Laporta, Jorge, (2002). Fundamentos de telemática. Editorial de la UPV. Valencia

[3] Tanenbaum, Andrew, (2003). Redes de computadoras. 4ed.Mexico, D. F. Pearson Educacion

[4] Paquet, Catherine y Teare, Diane, (2001). Creación de redes cisco escalables. Pearson Educacion, S.A., Madrid

[5] SHELDON Tom, LAN TIMES: Enciclopedia de redes networking, Mc Graw-hill, México, 1994.

[6] PARNELL Tere, LAN TIMES: Guía de redes de alta velocidad, Mc Graw-hill, Madrid, 1997.

[7] JENKINS Neil, Redes de área local, Prentice Hall, México, 1996.

[8] FORD Merilee, Tecnologías de interconectividad de redes, Prentice Hall, México, 1998.

[9] 3Com, 3COM Stackable switch family-advanced configuration guide, 3Com Corporation.

[10] Cisco Systems, Academia de networking de cisco systems guía del segundo año CCNA 3 Y 4, Pearson Educación, Madrid, 2004.

[11] Stallings, Williams (2000). Comunicaciones y redes de computadores. Madrid/ Prentice- Hall/ c2000

[12] McQuerry, Steve, (2004).Interconexión de dispositivos de red cisco libro de autoestudio CCNA 2ed. Pearson Educacion, S.A., Madid, 2004

[13] TIA/EIA STANDARD, (2001). Commercial Building Telecommunications Cabling Standard. TIA/EIA-568-B. Telecommunications Industry Association.

[14] TIA/EIA STANDARD, (2004). Commercial Building Standard for Telecommunications Pathways and Spaces. TIA/EIA-569-B. Telecommunications Industry Association.

[15] TIA/EIA STANDARD, (2002). Administration Standard for Commercial Telecommunications Infraestructure. TIA/EIA-606-A. Telecommunications Industry Association.

[16] TIA/EIA STANDARD, (2002). Commercial Building Grounding (Earthing) and Bonding Requirements For Telecommunications. J-STD-607-A. Telecommunications Industry Association.

[17] http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml

[18]http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf----vlan
[19] http://www.unsa.edu.pe/infounsa/cursor/01/cursor01.pdf
[20] http://es.kioskea.net/contents/internet/vlan.php3
[21]http://www.commserv.ucsb.edu/infrastructure/standards/history/EIA-TIA_568.asp
[22] http://www.dte.us.es/personal/mcromero/docs/arc1/tema2-arc1.pdf
[23] http://www.ansi.org/
[24]http://www.rfc-es.org/rfc/rfc1918-es.txt
[25] http://www.ecaus.org/eia/site/index.html
[26] http://www.alfinal.com/Temas/cableadoestructurado.php
[27]http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/CableadoEstructurado2.pdf
[28]http://www.tiaonline.org/standards/
[29] http://www.luguer.com/catalogos/pdf/DTX_ES.pdf
[30] http://www.flukenetworks.com/datacom-cabling/copper-testing/LinkWare-Stats
[31] http://h17007.www1.hp.com/us/en/index.aspx
[32] http://www.fingertec.com/images/w_brochure/AC900_e.html
[33] http://www.cisco.com

BIOGRAPHIES

Ramon I. Nancy Y. was born in Ibarra, Imbabura Province, on August 26, 1986. She attended elementary school in Ana Luisa Leoro School, and she received his secondary education at the Ibarra National College. She entered the Faculty of Engineering in Applied Science at the Northern Technical University in 2004, Race Engineering in Electronics and Communication Networks. She completed his apprenticeships at the Invetrónica Cia. Ltd company in the technical department, performing Antenna Design, Engineering Studies, Programming Radio Equipment and Repair Power Supply. At the Technical University - North Library Building performed tasks such as Analysis, Assessment, Certification and Rectification network ports. At the RedSoluciones Company she worked at Area Network, performing tasks such as Analysis and Network Design, L2 and L3 equipment Configuration, Network Information Gathering, Configuration, Administration and Training on Tools of Monitoring and Inventory IP and Management Network.

Carlos A. Vasquez A. was born in Quito, Pichincha Province, on September 19, 1981. He is an Engineer in Electronics and Telecommunications (CUM LAUDE), at National Polytechnic School (EPN) in Quito, Ecuador in 2008. He is currently Professor of the School of Engineering in Electronics and Communication Networks at the Technical University of Northern Ibarra, Ecuador, teaching subjects such as Networking II and III, Network Projects, Network Administration. He serves as lead vocal of the Academic Council of the School of Engineering in Electronics and Communication Networks. He passed the CCNA 1, 2, 3, 4 student courses in the period June 2006 - March 2007 in the National Polytechnic School and the CCNA 1 Instructor at the ESPOL, and he is studying for a Masters in Communication Networks (2nd Semester), at Pontificia Catholic University of Ecuador, Quito, Ecuador.