UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"REINGENIERÍA DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL (MIDENA)"

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

NANCY YOLANDA RAMÓN IBUJÉS

DIRECTOR: ING. CARLOS VÁSQUEZ

IBARRA –ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1002743928
Apellidos y Nombres	Ramón Ibujés Nancy Yolanda
Dirección	Isla Santa María #3-59 y Riobamba
Email	nancita2122@hotmail.com
Teléfono Fijo	06 2 545 776
Teléfono Móvil	090 311 503

DATOS DE LA OBRA	
Título	REINGENIERÍA DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL (MIDENA)
Autor	Ramón Ibujés Nancy Yolanda
Fecha	10 de abril de 2012
Programa	Pregrado
Título por el que se aspira	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Nancy Yolanda Ramón Ibujés, con cédula de identidad Nro. 1002743928, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 143.

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Nancy Yolanda Ramón Ibujés**, con cédula de identidad Nro. 1002743928, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, Artículos 4,5 y 6, en calidad de autora del trabajo de grado denominado **"REINGENIERÍA DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL (MIDENA)",** que ha sido desarrollado para optar por el título de: **Ingeniera en Electrónica y Redes de Comunicación,** quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en el formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

_____

Firma
Nombre: Nancy Yolanda Ramón Ibujés
Cédula: 1002743928
Ibarra a los 10 días del mes de abril de 2012

DECLARACIÓN

Yo, Nancy Yolanda Ramón Ibujés, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

Nancy Yolanda Ramón Ibujés

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Nancy Yolanda Ramón Ibujés, bajo mi supervisión.

Ing. Carlos Vásquez

DIRECTOR DEL PROYECTO

CERTIFICADO

Una vez revisado el CD, con el trabajo de grado de la Egresada: **Nancy Yolanda Ramón Ibujés**, con el tema del proyecto de titulación: **"REINGENIERÍA DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL (MIDENA)"**. El CD funciona en su totalidad.

Contenido del CD:

- Documento del Proyecto
  - Parte teórica
  - Parte experimental
  - Anexos
- Artículo Técnico

Atentamente:

Ing. Edison Jácome	Ing. Jaime Michilena	Ing. Milton López

MIEMBROS DEL TRIBUNAL

AGRADECIMIENTOS

Agradezco a Jehová Dios por guiar mi camino, brindarme fortaleza y cubrirme de bendiciones a lo largo de mi vida, a mis padres Ángel Ramón y Mirian Ibujés por su confianza, paciencia y amor brindado en todo momento, a mi hermano Freddy por su gran cariño y apoyo.

A la Universidad Técnica del Norte por su aporte en mi preparación y desarrollo tanto personal como profesional, a mi director de tesis el Ing. Carlos Vásquez por su valiosa colaboración para la culminación del presente trabajo, a todos sus catedráticos por los conocimientos y experiencias que han contribuído en mi desarrollo, en especial al Ing. Francisco Frey por su ayuda y apoyo brindado.

Al Ing. Hugo Chamba Gerente de RedSoluciones por auspiciar este trabajo de grado y brindarme además de las facilidades para su desarrollo, su apoyo y colaboración. Al Ministerio de Defensa Nacional por permitirme el acceso a sus instalaciones en las cuales se desarrolló la investigación a ser aplicada en el proyecto descrito, a todo su personal por la colaboración brindada en especial al Subs. Gonzalo Román y al Sgop. César Quiña por no solo darme su apoyo y ayuda para el desarrollo del presente trabajo sino también por ofrecerme su amistad. De igual manera agradezco a todos mis familiares y amigos quienes de una u otra manera me han ayudado a alcanzar un peldaño más en la vida y quienes han sido parte de un pilar fundamental en la misma.

Nancy

DEDICATORIA

A Jehová Dios gracias al cual existo, por darme el conocimiento y la capacidad para el desarrollo de éste proyecto de titulación. A mis padres Ángel y Mirian por brindarme su amor, apoyo y comprensión en todo momento de mi vida, por sus consejos y palabras de aliento brindadas en el momento adecuado, por su confianza depositada ante los retos presentados, porque me han enseñado que con dedicación, esfuerzo y entereza todas las metas pueden ser cumplidas.Y porque gracias a ellos, hoy soy lo que soy.

Nancy

Índice de Figuras

CAPÍTULO 1

CAPÌTULO 2

CAPÍTULO 3

CAPÍTULO 4

ANEXOS

Índice de Tablas

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El Ente del Ministerio de Defensa Nacional en estudio es uno de los organismos de planificación, dirección militar y asesoramiento permanente en políticas militares y de guerra. El servicio utilizado por medio de la red de datos de Fuerzas Armadas constituye un factor crítico ante la toma de decisiones en Pro de los Intereses Nacionales, por lo cual es importante que su infraestructura ofrezca alta disponibilidad y calidad de servicio, soportando grandes cantidades de tráfico, además de poseer escalabilidad, flexibilidad y seguridad.

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.

Para la aplicación del modelo jerárquico se realizó un estudio previo de las características del equipamiento existente bajo el cual posteriormente se estructura la nueva red y las configuraciones llevadas a cabo para el fin propuesto, teniendo también en cuenta criterios de apilamiento con lo que se eliminen las cascadas en la red, al manejarse varios switches como un switch más grande mejorando el rendimiento, flexibilidad y facilitando la administración de los mismos.

La microsegmentación de red en cambio está basada en el estudio de la estructura orgánica, funciones, roles y recursos compartidos de los usuarios, utilizando un direccionamiento eficiente VLSM, considerando además un rango de crecimiento en función de la cantidad de usuarios presentes en cada una de las subredes.

Así también la aplicación de seguridad tanto mediante la aplicación de un protocolo seguro de conexión con el equipamiento activo, como el control del tráfico generado en las diferentes vlan y el control a nivel de acceso a la red

ligando tanto la dirección MAC e IP brindan un nivel de seguridad adicional a la red, permitiendo limitar el tráfico en función de reglas para acceso establecidas.

Con el fin de asegurar la continuidad del servicio de red, la implementación de enlaces redundantes de conexión y la aplicación de un protocolo que asegure una topología libre de bucles, permite que la red se encuentre disponible a pesar de que alguno de sus enlaces físicos o equipos de conmutación fallen.

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.

Así, 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.

ABSTRACT

The Ministry of National Defense, entity under study, is one of the planning agencies, military leadership and ongoing advice on military policy and war. The service used by the data network of the Armed Forces is critical to making decisions in favor of national interests, so it is important to provide high availability infrastructure and service quality, supporting large amounts of traffic, besides having scalability, flexibility and security.

This paper proposes a design which improves the network performance, proposing a scheme based on a detailed study of its infrastructure and existing requirements through the application of a hierarchical model based on the study of layers, and the logic level network microsegmentation, as well as the implementation of a scheme that ensures continuity of service.

For the application of the hierarchical model was performed a preliminary study of the characteristics of existing equipment which subsequently under the new network structure and settings conducted for the purpose intended, taking into account criteria stacking thereby eliminate waterfalls in the network, multiple switches managed as a larger switch itself improve performance, flexibility and easier to manage them.

The network microsegmentation change is based on the study of the organizational structure, functions, roles and sharing resources of users, efficient routing using VLSM, also considering a range of growth based on the number of users present in each of subnets.

Well as application security by implementing a secure protocol to connect to the active equipment, such as control of traffic on different VLANs and access level control to the network linking both the MAC and IP provide a additional layer of security to the network, allowing to limit traffic based on access rules established. In order to ensure continuity of network service, the implementation of redundant connecting links and implementation of a protocol that ensures a loop free topology allows the network to be available even though some of its physical links or switching equipment failure.

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.

Thus, the development of this project provides an efficient solution for data network of the institution under which improves the performance and the service provided both to the different entities associated as to the internal network, considering the current infrastructure that counts it.

PRESENTACIÓN

El presente proyecto tiene como objetivo realizar el diseño de la reingeniería de la Red de Datos de un Ente del Ministerio de Defensa Nacional, con el cual se optimice el uso de la infraestructura por medio de la realización de una restructuración tanto a nivel físico como lógico de la red.

El modelo propuesto está basado en un modelo jerárquico de red por medio del cual se mejora las prestaciones del servicio brindado, además en el mismo se consideran características tales que se brinde alta disponibilidad sin dejar de lado la seguridad a nivel del equipamiento de networking.

En el primer capítulo se expone la fundamentación teórica concerniente a los campos de networking y cableado estructurado, revisando los organismos de estandarización, componentes de la red, modelos de comunicaciones y protocolos de enrutamiento, además de las características y componentes de un sistema de cableado estructurado, normativas y estándares vigentes.

En el segundo capítulo se detalla tanto el levantamiento de información de situación actual como el análisis de la misma, dentro de la cual se establecen las falencias y fortalezas de la red, sirviendo de base para el desarrollo del rediseño de red.

En el tercer capítulo se realiza el diseño de las topologías física y lógica, para lo cual previamente se revisan las políticas aplicadas en la red además de la proyección de crecimiento y los requerimientos obtenidos por parte de los usuarios. El desarrollo de la reingeniería de la red de datos de la institución está dado en función de las consideraciones de diseño a tomarse en cuenta para el cableado estructurado, políticas de administración para la parte activa, el modelo de red basado en una estructura jerárquica, así como la segmentación de red y el direccionamiento IP apropiados.

En el cuarto capítulo se muestra paso a paso las configuraciones necesarias para la aplicación del modelo de red propuesto, tanto las configuraciones enfocadas a cada capa del modelo como las configuraciones básicas que deben aplicarse a todo el equipamiento activo; adicionalmente se realiza la simulación

correspondiente, con el objetivo de demostrar la funcionalidad del modelo propuesto independiente de la tecnología utilizada, además del cumplimiento de los objetivos funcionales del mismo.

En el quinto capítulo se plasman las conclusiones y recomendaciones obtenidas del desarrollo y simulación del modelo de red, las mismas que deberán ser observadas durante el proceso aplicación, así como para la administración y gestión de la red.

Finalmente en los anexos se incluye el glosario de los términos utilizados en el presente proyecto, además de los archivos correspondientes al levantamiento de red, una muestra de la certificación del cableado estructurado realizado a nivel de recorridos horizontales, documentación con la nueva estructura de direccionamiento IP aplicado a nivel de usuarios y los archivos de configuración correspondientes al equipamiento de tecnología 3Com.

CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA

1.1 INTRODUCCIÓN

Este capítulo contiene la fundamentación teórica abarcada en el presente trabajo, el cual involucra los campos de las redes de comunicación y cableado estructurado. Su estudio previo brinda una idea general de los conceptos y parámetros que se manejan en el proyecto, permitiendo de esta manera comprender su contenido y dar una idea clara del mismo.

Para el desarrollo de este capítulo primero se comenzará con una revisión del área de redes de comunicación para posteriormente continuar con el ámbito de los sistemas de cableado estructurado.

1.2 ANTECEDENTES HISTÓRICOS DE LAS REDES [1], [17-21]

La historia de las redes comenzó en el año de 1957 cuando se creó en los Estados Unidos la Agencia de Investigación de Proyectos Avanzados ARPA[1], como un organismo afiliado al Departamento de Defensa con el fin de impulsar el desarrollo tecnológico; en sus inicios ARPA se dedicaba a la investigación de proyectos del tipo espacial y militar.

Posteriormente en el año de 1965 ARPA patrocinó un programa con el fin de analizar las redes de comunicación usando computadoras, este programa contaba con centros de investigación en varios lugares del país, los mismos que para comunicarse entre ellos contaban con un terminal que se conectaba directamente hacia las estaciones mediante una extensión, naciendo allí la idea de que una computadora pudiese conectarse hacia cualquier lugar sin necesidad de contar con conexiones directas como hasta el momento; de esa forma surge ARPANET[2].

[1] ARPA: Advanced Research Proyects Agency (Agencia de Investigación de Proyectos Avanzados).
[2] ARPANET: Advanced Research Proyects Agency Network (Red de la Agencia de Investigación de Proyectos Avanzados).

En 1969 se construyó la primera red ARPANET, constituida por cuatro nodos situados en la UCLA (Universidad de California en los Ángeles), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, Los Ángeles) y la Universidad de UTAH, los mismos que constituyeron la primera red. Posterior a esto se abrieron varios centros de investigación en cooperación con el Departamento de Defensa para promover el desarrollo de la misma, sin embargo los científicos que trabajaron en el proyecto comenzaron a utilizarlo con fines de comunicación y charla personal incluida la ciencia ficción, con lo cual surge la necesidad de separar la investigación con fines militares y de comunicaciones, formándose las redes MILNET[3] y ARPANET respectivamente. Adicional se crearon las redes CSNET[4] y BITNET[5], pero todas ellas usaban como backbone principal ARPANET.

ARPANET fue llamada luego ARPA-INTERNET y posteriormente INTERNET nombre con el cual se conoce en la actualidad a esta red de redes.

Con el surgimiento de la red también se introdujo un concepto muy importante, la velocidad de transmisión; en la década de los 70's se hablaba de transmisiones de unos miles de bits por segundo, posteriormente para los 80's se hablaba de millones de bits y en los 90's de decenas de millones de bits, sin embargo, era necesario tener en cuenta que se debía manejar un protocolo que sea soportado por los dos extremos tanto emisor como receptor, haciéndose necesario la creación de un protocolo de red que entiendan todas las redes. Como resultado se creó el protocolo TCP/IP[6] como estándar de comunicación entre computadores, modelo por el cual se basan las transmisiones en la actualidad.

1.3 IMPORTANCIA DE LAS REDES

Aunque en sus inicios el uso de las redes estuvo limitado para fines militares y de investigación ligados al proyecto ARPANET, poco a poco se fue extendiendo hacia la comunidad universitaria y luego hacia el público en general,

[3] MILNET: Military Network (Red Militar)
[4] CSNET: Computer Science Network (Red de Ciencias de la Computación)
[5] BITNET: Because It's Time Network (Red Porque ya es Hora)
[6] TCP/IP: Transmission Control Protocol / Internet Protocol (Protocolo de Control de Transmisión / Protocolo de Internet)

constituyéndose así en la actualidad en uno de los servicios más utilizados a nivel mundial.

Su uso no se limita a ciertas aplicaciones sino más bien, éste se ha popularizado tanto para aplicaciones en tiempo real, diferido y charlas personales permitiendo compartir recursos, programas, archivos, bases de datos, entre otros, de forma centralizada independiente del desarrollador de las PC´s.

Actualmente las redes de comunicación constituyen una parte fundamental para el desarrollo de las actividades diarias, pudiendo estas ser apreciadas de forma directa o indirecta, un ejemplo muy común de su uso son los servicios bancarios, pagos en línea, redes sociales, entre otros.

1.4 CONCEPTOS BÁSICOS DE REDES

Es muy importante comenzar con una revisión de los términos más utilizados en redes los cuales se describen a continuación.

1.4.1 TIPOS DE SEÑALES ELÉCTRICAS [22- 23], [29]

Las señales eléctricas se clasifican en dos tipos: analógicas y digitales, siendo su principal característica la forma de transmisión de la señal.

Señales Análogas:- Es una señal continua en el tiempo, cuyos valores cambian suavemente de un estado a otro dentro de un rango de valores determinados.

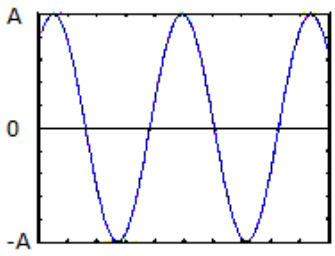


Figura 1. Señal analógica [3]

Señales Digitales:- Es una señal que está limitada a tomar ciertos valores discretos, utilizando una lógica binaria de 0 y 1. Una transmisión digital reduce el índice de errores durante una transmisión, ya que ésta se limita a tomar sólo valores determinados.

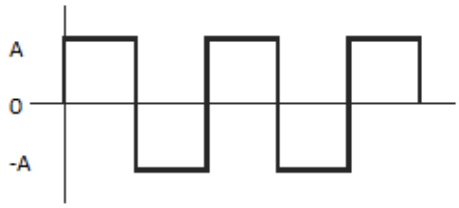


Figura 2. Señal digital [3]

En ambientes con ruido, el empleo de señales digitales puede resultar muy beneficioso ya que este tipo de señales permite ignorar ciertas variaciones de la misma y cualquier señal cercana a un valor umbral es considerada como dicho valor; sin embargo es necesario tener en cuenta que al convertir de una señal analógica a una señal digital, muchos valores pueden perderse dependiendo del nivel de cuantificación que se utilice, haciéndola más o menos eficiente.

1.4.2 TIPOS DE TRANSMISIÓN [24-25], [29]

Para que las transmisiones realizadas entre el emisor y receptor sean entendidas por los dos extremos, es necesario que ambos conozcan o entiendan cuando una transmisión a empezado y cuando ésta a finalizado; para ello es importante determinar el tipo de transmisión que utilizarán, pudiendo ser de dos tipos: asincrónica o sincrónica.

Asincrónica.- En este tipo de transmisión no se requiere tener una sincronización previa de los relojes del transmisor y receptor.

Para empezar una transmisión se utiliza bits especiales que indican el comienzo y final de cada caracter, a éstos se los conoce como bits de inicio o arranque y bits de final o parada. Los bits de inicio indican el comienzo de una transmisión, en cambio los bits de parada indican que ha concluido la transmisión dejando también así preparado el canal para una nueva transmisión; así mismo en este tipo de comunicación se utiliza un bit adicional de paridad, pudiendo ser par o impar, lo cual permite comprobar que los datos se hayan transmitido correctamente.

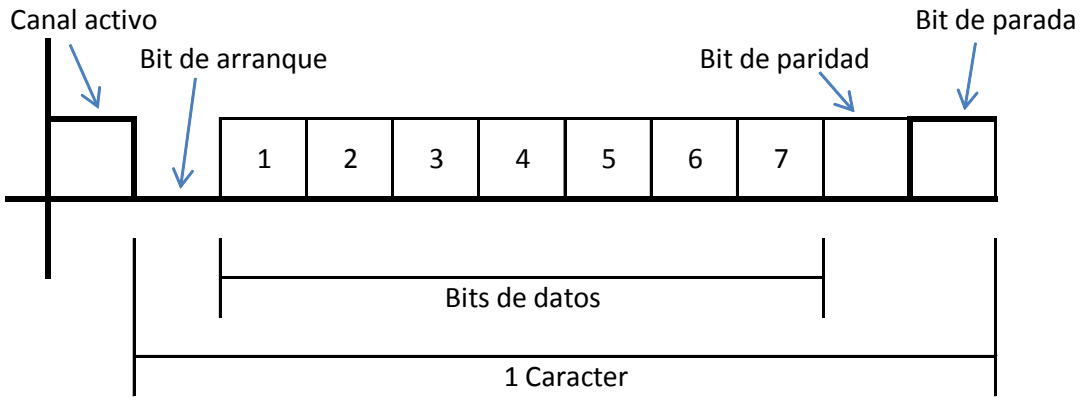


Figura 3. Transmisión asincrónica [24]

Se utilizan transmisiones asincrónicas cuando se requiere transmitir pequeñas cantidades de datos, ya que al necesitar incluir bits especiales para separar cada caracter hacen de este tipo de transmisión ineficiente para grandes cantidades de transmisión de datos. Sin embargo una de sus ventajas es la rápida recuperación de errores, ya que al transmitirse uno a uno si existen errores en la transmisión, solo se pierden pequeñas cantidades de datos.

Sincrónica.-En este tipo de transmisión es necesario que tanto los relojes del transmisor como del receptor se encuentren sincronizados antes de empezar una nueva transmisión; para delimitar cada bloque se utilizan los llamados bits delimitadores de bloque.

Al transmitirse la información por tramas, la transmisión se torna más eficiente permitiendo tener un flujo de datos más regular.

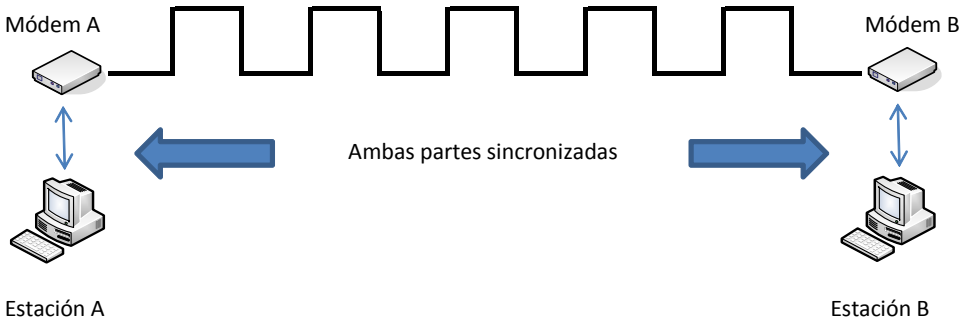


Figura 4. Transmisión sincrónica [26]

1.4.3 ANCHO DE BANDA [27-28]

El ancho de banda indica la cantidad de información o de datos que se puede transmitir en una unidad de tiempo determinada. Mediante este parámetro es posible determinar la velocidad de transmisión que tendrá la red y también así poder establecer cuál será el ancho de banda mínimo necesario para soportar todas las aplicaciones.

La unidad utilizada es bits por segundo (bps), aunque también se utilizan sus múltiplos como Kbps, Mbps o Gbps, dependiendo de la cantidad de bits que se transmitan.

El ancho de banda esta dado por un rango de frecuencias por el cual se transmite la información de un sistema en forma correcta.

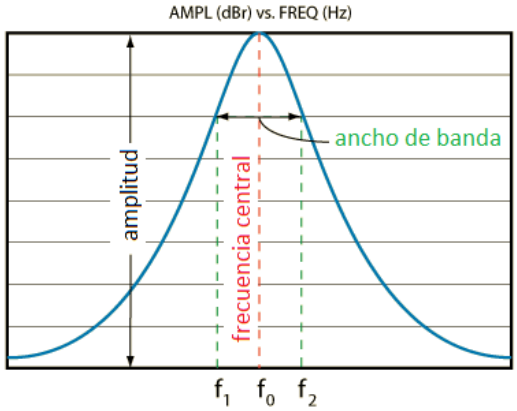


Figura 5. Ancho de banda [28]

1.4.4 DOMINIOS DE COLISIÓN Y DIFUSIÓN [12], [30]

Un dominio de colisión implica un segmento de red físico en el cual todos los dispositivos conectados a la red forman parte de un mismo dominio de colisiones, si dos de ellos intentan acceder al canal a la vez producirán colisiones, afectando directamente al desempeño de la red. Al aumentar estaciones que compartan el mismo segmento de red, aumenta también la posibilidad de que se generen colisiones en el canal.

En cambio un **dominio de difusión** constituye un grupo de estaciones o dispositivos en una red que reciben los mensajes de difusión o broadcast de los demás, es decir de todos los dispositivos que forman parte de la misma red

lógica. Una cantidad inapropiada de éstos produce un bajo rendimiento en la red o incluso podría generar una congestión total en la misma.

En la figura 6 se puede distinguir la diferencia entre un dominio de difusión y colisión que se crean dependiendo de los equipos de red que se utilicen.

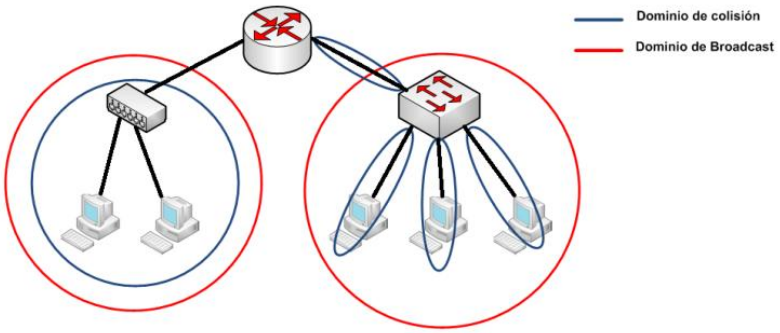


Figura 6. Dominios de colisión y dominios de difusión [30]

1.4.5 TOPOLOGÍAS DE RED [11], [29], [31-36]

Las topologías de red indican la forma en que se encuentran interconectados los equipos y la forma en que la información es transmitida.

Tipo Bus.- Las estaciones de trabajo se conectan a un único canal físico de comunicación una a continuación de otra. La comunicación se realiza mediante broadcast, propagándose a través de todo el medio de comunicación.

Al ser una comunicación del tipo lineal es necesario adicionar terminadores de red en los extremos del canal de comunicación para evitar rebotes de la señal.

En este tipo de topología su implementación es más barata ya que no necesita equipos intermedios para su interconexión, pero dentro de sus principales desventajas es que al producirse algún fallo en el canal de comunicación, la red quedaría total o parcialmente fuera de servicio.

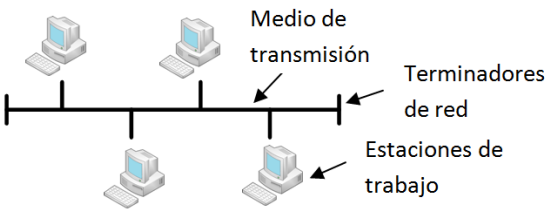


Figura 7. Topología tipo bus [3]

Tipo Anillo.- El medio de comunicación de una red tipo anillo se constituye como un lazo cerrado, el cual integra a todas las estaciones de trabajo. La información se transmite de una estación a otra en una sola dirección, debiendo pasar por todas las estaciones intermedias que forman parte de la topología.

En este tipo de topología no es necesario tener terminadores de red ya que no existe un punto final. Se la considera a esta topología como activa, ya que la señal es regenerada en cada estación de trabajo por la cual pasa la comunicación.

Al producirse algún fallo en la red, no necesariamente toda la red quedará fuera de servicio ya que solo la parte defectuosa será aislada de la misma.

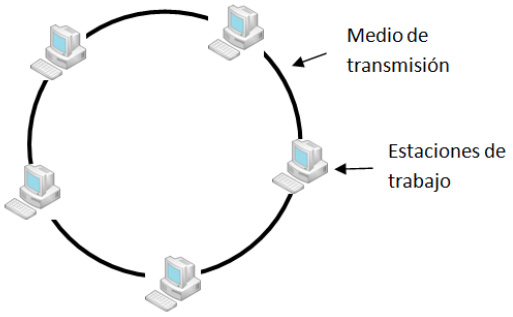


Figura 8. Topología tipo anillo [3]

Tipo estrella.- Una red de este tipo se caracteriza por tener un nodo central al cual se conectan las demás estaciones y todas las comunicaciones se realizan a través de éste. En esta topología el añadir o extraer estaciones resulta muy fácil y no interrumpe el normal funcionamiento de la red, al producirse fallos en alguna estación de trabajo solo la estación defectuosa quedaría aislada.

Su principal desventaja radica en el nodo central, ya que si éste falla toda la red quedaría incomunicada debido a que todas las estaciones se conectan directamente a él.

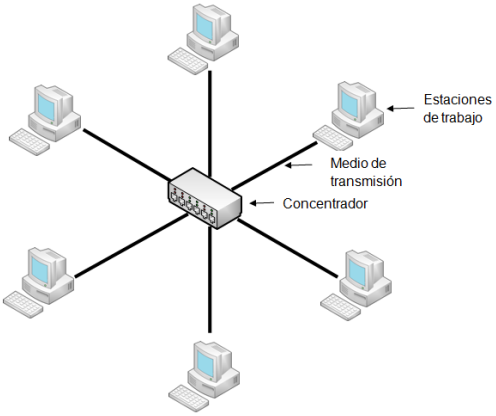


Figura 9. Topología tipo estrella [3]

A las topologías anteriormente indicadas se las considera topologías puras, las demás topologías generadas están conformadas por la unión de ellas.

1.4.6 CLASIFICACIÓN DE LAS REDES [12], [29], [37-39]

Las redes de comunicación se pueden clasificar dependiendo de su cobertura geográfica en redes LAN[7], WAN[8] y MAN[9], a continuación se describen cada una de ellas.

1.4.6.1 Redes de Área Local - LAN (*Local Area Network*)

Una red LAN comprende una cobertura moderada pudiendo abarcar un edificio o incluso la interconexión entre dos de ellos, permitiendo compartir recursos e intercambiar información, manejando bajos tiempos de retardo y con un mínimo de errores de transmisión.

Una red LAN incluye tanto las topologías, el medio de transmisión y la forma de acceso al medio. La tecnología que soporta la infraestructura de una red LAN está basada en el protocolo Ethernet.

1.4.6.1.2 Redes LAN Virtuales - VLAN[10] (Virtual Local Area Network)

Las VLAN permiten dividir a una red en varias subredes segmentadas lógicamente. Mediante la creación de VLAN es posible agrupar a los usuarios que tengan funciones similares independientemente de su ubicación física, permitirles

[7] LAN: Local Area Network (Redes de Área Local)
[8] WAN: Wide Area Network (Red de Área Extensa)
[9] MAN: Metropolitan Area Network (Red de Área Metropolitana)
[10] VLAN: Virtual Local Area Network (Redes de Área Local Virtuales)

movilidad y mayor seguridad, así también se limita los dominios de broadcast entre los miembros de la VLAN, ya que el tráfico únicamente se trasmite entre ellos, es decir, al disminuirse el tráfico que circula en la red aumenta el rendimiento de la misma.

1.4.6.2 Redes de Área Extensa - WAN (*Wide Area Network*)

Las redes de área extensa (WAN) surgen por la necesidad de brindar interconexión a redes de lugares geográficamente dispersos. Estas redes comprenden una mayor extensión que una red LAN, permitiendo a las mismas su interconexión y el acceso a los servicios que provee la red, formando una conexión del tipo punto a punto.

En este tipo de redes los tiempos de retardo aumentan en relación a una red LAN dependiendo de varios factores, como el medio de transmisión a utilizarse, la velocidad de transmisión, entre otros.

1.4.6.3 Redes de Área Metropolitana MAN (Metropolitan Area Network)

Una red MAN es utilizada para interconectar redes LAN cercanas, las mismas que además utilizan una tecnología similar lo que permite que nodos remotos se comuniquen como si formaran parte de la misma red.

Cabe indicar que actualmente esta clasificación no se la utiliza, distinguiéndose simplemente las redes LAN y WAN.

1.5 ORGANISMOS DE ESTANDARIZACIÓN DE REDES [40-44]

Dentro de los organismos de estandarización de redes se encuentran la ISO[11], IEEE[12], IETF[13] y la ITU[14], éstos han desarrollado diferentes protocolos y estándares de interés para el establecimiento de redes y la aplicabilidad que se les desea dar.

ISO.- La Organización Internacional de Estándares (International Standards Organization) es una organización no gubernamental cuya función se centra en el desarrollo y publicación de estándares de calidad, con la finalidad de facilitar el comercio a nivel mundial en lo relacionado a bienes y servicios, desarrollo científico, intelectual, tecnológico y económico.

IEEE.- El Instituto de Ingenieros Eléctricos y Electrónicos (The Institute of Electrical and Electronics Engineers) es una sociedad que desarrolla estándares para las industrias eléctricas y electrónicas particularmente en el área de redes de datos. El IEEE promueve la creatividad, el desarrollo y la integración, además comparte y aplica los avances en las tecnologías de la información, electrónica y ciencias en general.

IETF.- El Grupo de Trabajo en Ingeniería de Internet (Internet Engineering Task Force) es una organización internacional abierta de normalización, cuyo fin es contribuir a la ingeniería de Internet y lo desarrolla a nivel técnico mediante la creación, prueba e implementación de estándares, además el IETF tiene la autoridad para establecer modificaciones de los parámetros técnicos sobre los que funciona la red. Su misión es velar porque la arquitectura de la red y los protocolos técnicos funcionen correctamente.

[11]ISO: International Standards Organization (Organización Internacional de Estándares)
[12]IEEE: The Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)
[13]IETF: Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet)
[14]ITU: International Telecomunication Union (Unión Internacional de Telecomunicaciones)

UIT.- La Unión Internacional de Telecomunicaciones (International Telecomunication Union) es el principal organismo de las Naciones Unidas en cuestiones relacionadas a tecnología de información y comunicación, además, en la UIT los gobiernos y el sector privado coordinan las redes y los servicios mundiales de telecomunicaciones.

Su objetivo es estudiar y definir recomendaciones de cuestiones técnicas, tecnológicas, de operación y tarifación en el sector de las telecomunicaciones brindando así una compatibilidad de extremo a extremo en las conexiones internacionales. Además permite un fácil y asequible acceso a la información y comunicación contribuyendo al desarrollo económico y social de las personas.

1.6 COMPONENTES DE UNA RED

Para implementar una red no basta con tener las estaciones de trabajo sino también es necesario contar con el medio de transmisión y el/los componentes de red activos que permitan configurar la misma. A continuación se describen los componentes necesarios para ello.

1.6.1 MEDIOS DE TRANSMISIÓN GUIADOS

Dentro de los medios de transmisión guiados se pueden diferenciar los basados en cobre y los basados en fibra óptica, cada uno de ellos se los utiliza en base a las características de transmisión deseadas, costos y aplicabilidad necesarias.

1.6.1.2 Medios de Transmisión Basados en Cobre [3], [11-12], [31], [46-47]

Los medios de transmisión basados en cobre se dividen básicamente en dos: cable coaxial y cable par trenzado, sin embargo es necesario conocer los subtipos que tienen los mismos, ya que dependiendo del medio y su aplicación éstos son utilizados.

Cable coaxial.- Este tipo de cable está conformado por un hilo central rodeado por una malla de hilos de cobre, los mismos que se encuentran separados por un material dieléctrico y a su vez todo se encuentra protegido por un material aislante.

Este tipo de cable presenta características favorables ante la interferencia electromagnética, sin embargo su manipulación debido a la rigidez y la alta atenuación en base a su longitud son parte de sus principales desventajas.

El cable coaxial banda base utilizado en redes Ethernet tiene una impedancia característica de 50 ohmios, razón por la cual se lo suele utilizar para televisión, telefonía, conexión de periféricos de corta distancia y redes de computadores, aunque en la actualidad su uso en redes Ethernet se encuentra descontinuado.

Cable Par Trenzado.- Este tipo de cable está formado por pares de hilos de cobre aislados por una cobertura plástica y trenzados entre sí. El trenzado entre los pares elimina el ruido electrónico de los pares adyacentes y de fuentes externas.

El cable par tranzado se subdivide en cable par trenzado UTP[15], STP[16] y FTP[17].

UTP o **Cable trenzado sin apantallar***:* Es muy utilizado en redes Ethernet y telefonía debido a su flexibilidad y bajo costo de instalación. Este tipo de cable tiene una impedancia característica de 100 ohmios.

FTP o **Par trenzado con pantalla global***:* Este tipo de cable cuenta con una pantalla global que brinda una protección adicional ante las interferencias electromagnéticas externas y su impedancia característica es de 120 ohmios.

STP o **Par trenzado apantallado**: en este tipo de cable cada uno de sus pares cuenta con una pantalla metálica, la cual brinda protección ante las interferencias y el ruido eléctrico muy superiores a las ofrecidas por el cable UTP, sin embargo, el contar con pantallas individuales hacen a este cable más rígido, costoso y con mayor dificultad para su instalación. Su impedancia característica es de 150 ohmios.

A continuación se muestra una figura de los diferentes medios de transmisión basados en cobre.

[15]UTP: Unshielded Twisted Pair (Cable Trenzado sin Apantallar)
[16]STP: Shielded Twisted Pair (Par Trenzado Apantallado)
[17]FTP: Foiled Twisted Pair (Par Trenzado con Pantalla Global)

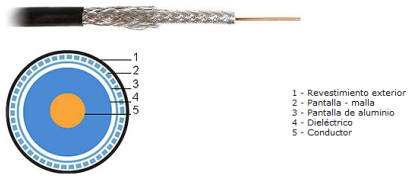
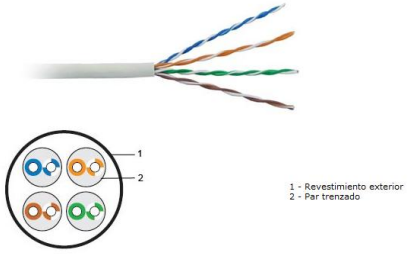
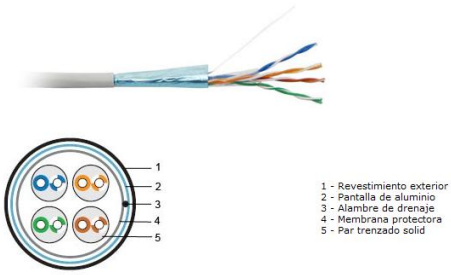
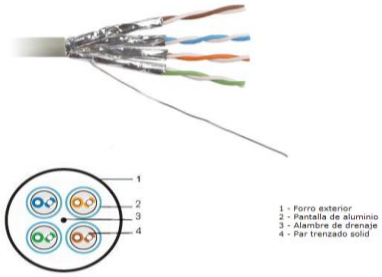
Cable coaxial	Cable trenzado sin apantallar
	
Par trenzado con pantalla global	**Par trenzado apantallado**
	

Figura 10. Medios de transmisión basados en cobre [45]

1.6.1.3 Medios de Transmisión Basados en Fibra Óptica [3], [11-12], [50]

La fibra óptica es un medio de transmisión formado por un filamento de vidrio o plástico, recubierto por un material aislante, que protege a la fibra óptica. Su forma de transmisión es por medio de ondas de luz, haciéndola esto inmune a las interferencias electromagnéticas y al ruido del medio. El uso de la fibra óptica permite alcanzar grandes distancias y velocidades de transmisión muy altas, convirtiéndole en un medio muy utilizado para la interconexión de redes LAN o WAN; sin embargo uno de sus principales limitantes es su elevado costo de instalación en comparación con otros medios de transmisión guiados, haciendo de esta inapropiada para el uso e instalación en distancias pequeñas.

Los sistemas de fibra óptica se pueden clasificar en fibras multimodo y fibras monomodo. Una fibra óptica monomodo contiene un único haz de luz que se propaga en el medio, lo cual le permite alcanzar mayores distancias y velocidades; en cambio una fibra óptica multimodo está conformada por múltiples haces de luz que viajan por un mismo medio de transmisión pero con ángulos de reflexión diferentes lo cual limita su distancia y velocidades de trasmisión.

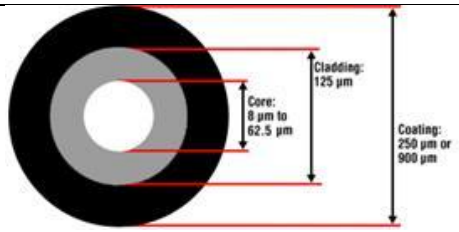
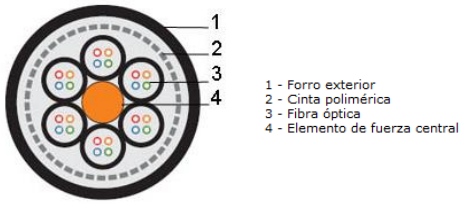
Fibra óptica Monomodo	Fibra óptica Multimodo
	

Figura 11. Medios de transmisión basados en fibra óptica [45]

1.6.2 MEDIOS DE TRANSMISIÓN INALÁMBRICOS O NO GUIADOS [3], [11-12], [46], [48-49]

Los medios de transmisión inalámbricos para propagarse por el espacio utilizan ondas electromagnéticas, siendo su principal medio de transmisión el aire, así mismo para su transmisión y recepción utilizan antenas programadas en frecuencias específicas.

Este tipo de medio de transmisión es muy utilizado en lugares de difícil acceso o en zonas en las cuales no es viable o adecuada la instalación de cable ya que además permite alcanzar grandes distancias y brindar movilidad.

A todo el rango de frecuencias utilizado por las transmisiones inalámbricas se lo denomina espectro electromagnético, el mismo que es administrado y regulado por el Estado; en la siguiente figura se muestra un cuadro con la distribución del espectro electromagnético y su uso.

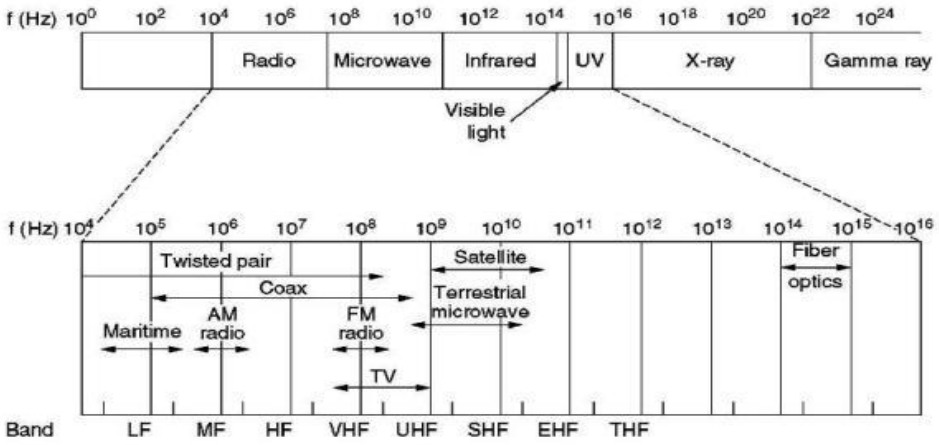


Figura 12. Distribución del espectro electromagnético [51]

Se pueden distinguir diferentes tipos de transmisiones inalámbricas dependiendo de la banda de frecuencias que se utilice, la misma que determina características especiales de cada transmisión.

Radiofrecuencias.- son muy utilizadas en viviendas, sistemas domóticos y de telemando, para su operación no es necesario obtener licencias pero si respetar los límites de potencia de transmisión. En su trasmisión se utilizan bandas ISM[18], lo cual las hace susceptibles a interferencias y a una fácil intervención de las comunicaciones.

Infrarrojos.- se las utiliza para transmisiones de corta distancia y al igual que los sistemas de radiofrecuencia no requieren licenciamiento para su utilización. Estos sistemas se transmiten en línea recta y no pueden traspasar los objetos sólidos, lo cual brinda una ventaja a este sistema ya que reduce la posibilidad de que se presenten interferencias por sistemas contiguos. Son utilizados principalmente al interior de viviendas u oficinas.

Microondas.- son utilizados para comunicaciones de larga distancia, para lo cual se requiere tener línea de vista, haciéndose necesario la mayoría de veces instalar las antenas sobre torres para establecer comunicación entre dos puntos distantes sin que existan obstáculos en su trayectoria. Este tipo de transmisiones pueden verse afectadas por factores atmosféricos o por la topografía del terreno y su explotación requiere tener un licenciamiento previo. Son muy utilizados para enlaces punto a punto o como backups de los sistemas de red cableados.

Satelitales.- son muy utilizados para abarcar grandes distancias ya que cubren toda el área de cobertura que tenga el satélite, haciéndolo independiente de su ubicación geográfica. Una de sus desventajas es el retardo que sufren las comunicaciones, pudiendo acentuarse dependiendo de la órbita en la que se encuentre el satélite. Son utilizados tanto para enlaces punto a punto como multipunto.

[18] ISM: Industrial, Scientific and Medical (Industrial, Científica y Médica)

1.6.3 COMPONENTES ACTIVOS [12], [31]

Para que una red pueda funcionar correctamente a más de tener un enlace físico necesita de varios equipos o dispositivos que permitan brindar el servicio, es importante diferenciarlos ya que dependiendo de los requerimientos y características de la red se deberá utilizar uno u otro equipamiento. Dentro de los principales se tiene:

Repetidores.- son dispositivos que trabajan a nivel físico y regeneran eléctricamente la señal para permitir alcanzar mayores distancias. Estos dispositivos repiten todos los bits sin examinar su contenido, por lo cual son considerados elementos no inteligentes, pudiendo causar dominios de colisión en la red al no discriminar el tráfico de un segmento u otro.

Los repetidores son utilizados para interconectar dos segmentos con diferentes medios físicos siempre y cuando estos manejen los mismos protocolos de comunicación, así también estos son empleados para extender la longitud de los segmentos de red.

Figura 13. Repetidor VLR104 [31,5]

Hubs.- son dispositivos que permiten extender una red LAN, facilitando interconectar segmentos de red con diferente medio físico.

Es considerado como un repetidor multipuerto ya que este dispositivo repite la misma señal por cada uno de sus puertos, excepto en el que ha recibido el paquete, de forma que todos los puertos tienen acceso a los datos, formando también así un dominio de colisión y un dominio de broadcast independiente. Los hubs de igual forma que los repetidores no discriminan el tráfico de red cursante; estos además se encargan de enviar una señal de choque a todos los puertos cuando se detecta una colisión.

Los hubs constituyen la base para las redes de topología tipo estrella.

Figura 14. HUB 3Com Office Connect [64]

Switch.- estos dispositivos permiten interconectar redes LAN a nivel de la capa de enlace, es decir que estos elementos examinan las direcciones MAC[19] de las tramas destino durante la transmisión de paquetes.

Un switch forma un dominio de broadcast y cada uno de sus puertos forman un dominio de colisión, de ésta manera se permite mejorar el rendimiento y seguridad de las redes LAN.

Cabe indicar que los switch a los que se hace referencia son de capa dos, ya que también existen switches de capa tres los cuales realizan funciones de ruteo.

Figura 15. Switch 3Com 4210G [64]

Router.- son dispositivos que permiten interconectar varios segmentos de red y controlar el tráfico que se genera entre ellos independientemente del protocolo que ellos manejen. Los ruteadores trabajan a nivel de capa de red, es decir que pueden decidir la línea de salida de los datos en base a su IP y tabla de ruteo. Los routers son dispositivos que separan tanto los dominios de broadcast como los dominios de colisión.

Figura 16. Router 3Com A6600 [64]

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

1.7 MODELOS DE COMUNICACIONES [3-4], [8], [12]

Para definir la forma en que se intercambia información entre dos sistemas computacionales es necesario estandarizar las funciones a realizar, siendo el propósito de los modelos de comunicaciones definir la implementación, estructuración y desarrollo que permite el dividir por capas las tareas relacionadas a una transmisión, por medio de lo cual se delegan tareas específicas a cada una de las capas logrando que los sistemas manejen una estructura por módulos y no que se maneje como un todo. Dentro de los modelos de comunicaciones se destacan dos: Modelo OSI[20] y Modelo TCP/IP.

El modelo OSI es un modelo de red con un fin teórico, un modelo de red descriptivo que constituye un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones; en cambio la Familia de Protocolos de Internet TCP/IP, es una implementación real de protocolos, diseñado como la solución a un problema práctico de ingeniería.

1.7.1 MODELO DE REFERENCIA OSI (Open System Interconnection) [3-4], [8], [11-12], [53], [54]

El modelo de referencia OSI permite entender de mejor manera el funcionamiento de una red y la manera en que fluye el tráfico en la misma, además este modelo sirve como una guía para la creación de estándares, esquemas y dispositivos de red.

El modelo OSI permite la interoperabilidad entre sistemas de diferentes fabricantes, por lo que un sistema puede ampliarse o adaptarse con otros sistemas, además al manejar una estructura por capas brinda una mayor simplicidad, ya que separa las diferentes funciones de red permitiendo también definir protocolos más sencillos.

El modelo OSI se encuentra conformado por siete capas que son:

[20] OSI: Open System Interconnection (Interconexión de Sistemas Abiertos)

Figura 17. Capas del Modelo OSI [52]

1.7.1.1 Capa Física

La capa física es la encargada de transmitir la información en un lenguaje binario por el medio de comunicación debiendo garantizar la conexión.

Esta capa se encarga de definir las características mecánicas, eléctricas, funcionales y de procedimiento que se utilizarán en una transmisión.

1.7.1.1.1 Características Mecánicas, Eléctricas, Funcionales y de Procedimiento

Las características mecánicas definen las propiedades físicas de la interfaz y del medio de transmisión, como tipo de cable, conectores, entre otros; las eléctricas en cambio definen la forma en que se representarán los bits y su velocidad de transmisión. Los aspectos funcionales indican las funciones que tendrá cada circuito de la interfaz física entre el sistema y el medio de transmisión, como los pines para transmisión (Tx) y recepción (Rx), además de las características procedurales, indicando los eventos que harán posible la activación o desactivación del canal.

1.7.1.1.2 Medios de Transmisión

Los medios de transmisión utilizados para transmitir información pueden ser:

- Guiados.- como cable coaxial, cable par trenzado o fibra óptica y/o
- No guiados.- como infrarrojos, radiofrecuencias, microondas o satelitales. *Ver. 1.6.1 Medios de transmisión guiados y 1.6.2 Medios de transmisión inalámbricos.*

1.7.1.1.3 Tratamiento de Errores

Todo medio de comunicación está expuesto a errores en la transmisión producidos por fuentes externas, componentes electrónicos, el medio de transmisión, entre otros. Dentro de los errores más conocidos se pueden describir los siguientes:

Ruido.- Es una señal no deseada que se mezcla con la señal útil que se va a transmitir. Dependiendo del nivel de ruido en el canal, éste puede producir errores al interpretarse la información enviada. Aunque el ruido es imposible erradicar, se pueden establecer niveles de ruido aceptables, para lo cual la potencia de la señal debe ser mayor que la potencia del ruido.

Interferencia.- La interferencia también puede ser considerada como otro tipo de ruido, sin embargo cuando estas señales coinciden en fase provocan la superposición de dos o más ondas, generando una modificación o incluso la anulación de la señal emitida. Es decir, interferencia se considera a cualquier procedimiento que altera, modifica o destruye a una señal durante su transmisión.

Diafonía.- La diafonía se presenta cuando parte de la señales de un sistema aparecen en el otro. Esta se produce generalmente en sistemas de igual naturaleza, produciéndose un acoplamiento magnético entre los componentes de los dos sistemas.

Atenuación.- La atenuación es considerada como la pérdida de potencia de la señal, principalmente puede ser causada por la distancia que debe recorrer una señal, ésta es una característica propia del medio de transmisión.

Distorsión.- Se produce distorsión en una señal cuando parte de ella llega desfasada, produciéndose deformaciones y por ende mala calidad de la señal. Si se tienen desfases de 180 grados pueden producirse incluso pérdidas de la señal.

1.7.1.1.4 Modos de transmisión [54]

En una transmisión se pueden tener diferentes modos de transmisión dependiendo del sentido de transmisión y su simultaneidad:

Modo simplex: las señales se transmiten en un solo sentido.

Figura 18. Modo de transmisión simplex

Fuente: Nancy Yolanda Ramón I.

Modo semi-duplex o half-duplex: las señales se transmiten en ambos sentidos pero no de forma simultánea.

Figura 19. Modo de transmisión semi-duplex

Fuente: Nancy Yolanda Ramón I.

Modo full-duplex: las señales se transmiten en ambos sentidos y de forma simultánea.

Figura 20. Modo de transmisión full-duplex

Fuente: Nancy Yolanda Ramón I.

1.7.1.2 Capa de Enlace

Esta capa es la encargada de proporcionar la comunicación entre dos estaciones de trabajo, además de manejar el envío de mensajes desde la capa física a la capa de red y viceversa. Esta capa además es la encargada de asegurar que la información se encuentre libre de errores en la transmisión.

La capa de enlace de datos ya no maneja la información por bits sino más bien la agrupa en tramas para luego pasarla a la capa superior; si la información viene del lado contrario debe en cambio dividir la información.

Esta capa es la primera capa lógica que pertenece a este modelo, ya que maneja un direccionamiento físico, control y detección de errores, integridad de los datos y acceso a la capa de red. La capa de red agrupa la información en tramas agregándole además bits de control que permiten determinar la integridad de la comunicación y en caso de que ésta falle deberá pedir que se reenvíe el datagrama corrupto.

1.7.1.2.1 Direccionamiento MAC

Permite a una máquina fuente determinar la identidad de una máquina destino, ya que la dirección física de cada NIC[21] es única en el mundo y cada dispositivo de red tiene una dirección MAC. Esta dirección física está formada por 48 bits expresados en 12 dígitos hexadecimales como se puede observar en la figura:

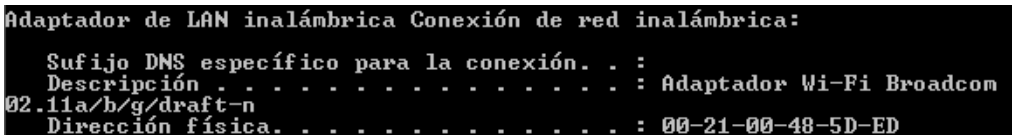


Figura 21. Vista de una dirección física

Fuente: Terminal de comandos PC-Nancy

1.7.1.2.2 Entramado

La unidad de datos utilizada en esta capa son las tramas, las cuales contienen además de la información de bits de control, bits que indican el comienzo y el final de la comunicación pudiendo para esto utilizarse varios métodos como conteo de caracteres, bits delimitadores o violaciones de código.

1.7.1.2.3 Subcapas de la capa de Enlace

La capa de enlace se subdivide en dos subcapas que son MAC y LLC[22], las cuales se describen a continuación:

[21] NIC: Network Interface Card (Tarjeta de Interfaz de Red)
[22] LLC: Logical Link Control (Control de Enlace Lógico)

Media Access Control ó Control de Acceso al Medio.- La subcapa MAC es la responsable del modo en que los datos se transmiten en el medio físico.

Esta capa define funciones como el direccionamiento físico, la topología de red, la notificación de errores, la distribución ordenada de tramas y el control de flujo.

El mecanismo de acceso al medio utilizado en redes Ethernet es CSMA/CD[23], el cual mejora las prestaciones de la red al verificar primero el estado del canal antes de empezar una nueva transmisión y verificar si se han producido colisiones.

Link Logic Control ó Control de Enlace Lógico.- La subcapa LLC provee a la capa de red una interfaz independiente de la tecnología aplicada en la capa de enlace y en la capa física.

Esta capa es la encargada de identificar lógicamente los tipos de protocolos y luego encapsularlos para su posterior transmisión; además maneja control de errores y control de flujo en la capa superior.

1.7.1.2.2 Tecnologías IEEE 802x

Las tecnologías IEEE 802 fueron creadas por el Instituto de Ingenieros Eléctricos y Electrónicos, desarrollando una serie de estándares, los mismos que especifican tanto las técnicas de acceso al medio como las diferentes opciones de transmisión.

Dentro de los protocolos de área local IEEE 802 el más utilizado es 802.3, que define las especificaciones del protocolo Ethernet, por lo cual se ampliará básicamente este protocolo.

IEEE802.3 Ethernet

La técnica de control de acceso al medio más ampliamente utilizada en redes Ethernet es la de acceso múltiple por detección de portadora con detección de colisiones CSMA/CD.

[23] CSMA/CD: Carrier Sense Multiple Access with Collision Detection (Acceso Múltiple por Detección de Portadora con Detección de Colisiones

Esta técnica de acceso al medio se la conoce como de acceso aleatorio o de contención; aleatorio ya que no tienen un tiempo establecido para iniciar una transmisión, este se realiza de forma aleatoria; y de contención debido a que las estaciones deben competir por el uso del canal.

Su funcionamiento se basa en que cuando una estación desea transmitir primero deberá escuchar el canal, y si este se encuentra libre la estación puede empezar a transmitir, caso contrario debe esperar hasta que el canal se libere para luego transmitir. Sin embargo en caso de que el canal se encuentre libre y dos estaciones transmitan simultáneamente se producirá una colisión, para lo cual se envía una señal de alerta “jam”, indicando a las demás estaciones el acontecimiento y que éstas dejen de transmitir, luego de esto las estaciones esperan un tiempo aleatorio para intentar volver a transmitir.

Dentro del protocolo Ethernet se especifican las diferentes opciones de transmisión como se detalla a continuación:

IEEE 802.3 a 10Mbps

Dentro del protocolo IEEE 802.3 se han desarrollado diferentes variantes como:

- 10BASE5
- 10BASE2
- 10BASE-T
- 10BASE-F

  Donde el número indica la cantidad de Mbps que se transmiten, la palabra BASE indica que se utiliza una señalización banda base, y las letras indican el medio utilizado (T=par trenzado, F=fibra óptica).

10BASE5.- utiliza cable coaxial RG-11 de 0,4 pulgadas de 50 ohmios, su longitud máxima permitida es de 500m, pudiendo extenderse con el uso de repetidores, máximo hasta 4 repetidores entre dos estaciones. Dentro de sus desventajas está el alto costo de los transceptores, poca flexibilidad debido a que se utiliza un cableado grueso y elevado costo.

10BASE2.- utiliza cable coaxial RG-58 de 0,2 pulgadas de 50 ohmios, su longitud máxima permitida es de 185m, pudiendo extenderse hasta con cuatro repetidores entre dos estaciones, aunque el tipo de cable utilizado es más fino continúa siendo poco flexible y con un alto costo.

10BASE-T.- emplea cable UTP, utilizado en topologías tipo estrella con una longitud máxima de 100m, para cualquier tipo de instalación nueva se recomienda la categoría 5e o superior. Su instalación es fácil debido a la flexibilidad del cable, así también la adición de nuevas estaciones no produce cortes de servicio, además de presentar una menor sensibilidad a fallas locales.

FOIRL.- fue el estándar original de fibra óptica para una red Ethernet, diseñado para los enlaces entre repetidores de no más de 1Km, luego éste fue remplazado por el estándar 10BASE-FL.

10BASE-F.- utiliza como medio de transmisión fibra óptica, dentro del estándar se distinguen las siguientes especificaciones:

- **10BASE-FL**.- permite la conexión entre dos repetidores, dos computadores o entre un repetidor y una computadora, con enlaces de hasta 2Km. Los enlaces que se definen en este protocolo son punto a punto.

- **10BASE-FB**.- utilizada como una solución de redes de backbone de fibra óptica. 10BASE-FB permite incrementar el número de repetidores en una red Ethernet de 4 a 12.

- **10BASE-FP**.- conocido como sistema de fibra óptica pasivo, emplea un acoplador en estrella pasivo permitiendo conectar hasta 33 estaciones de trabajo con una longitud de hasta 500m. Esta especificación se desarrolló con el objetivo que la fibra óptica llegue hasta la misma estación de trabajo, sin embargo esta especificación no fue aceptada debido a su costo.

1.7.1.3 Capa de Red

La capa de red es la encargada de definir la forma en que se transporta el tráfico entre estaciones finales, preocupándose de que el paquete llegue a su destino.

Este nivel se encarga de realizar un direccionamiento lógico además del enrutamiento necesario para que los paquetes alcancen su destino.

1.7.1.4 Capa de Transporte

Proporciona la interconexión entre dos sistemas finales, estableciendo conexiones lógicas entre las capas de transporte de dos sistemas de extremo a extremo.

La capa de transporte se asegura de que los mensajes lleguen correctamente y sin errores hacia el destino, así mismo permite el ensamblado y desensamblado de los segmentos de la capa de sesión hacia la capa de red, asegurándose que cada uno de los segmentos lleguen en un orden correcto y sin errores.

1.7.1.5 Capa de Sesión

Esta capa permite establecer, administrar y finalizar sesiones entre los usuarios de los diferentes host.

1.7.1.6 Capa de Presentación

En esta capa se define el formato y la semántica de los datos a transmitir.

1.7.1.7 Capa de Aplicación

Por medio de esta capa se brinda el acceso de las aplicaciones a los servicios de las demás capas del modelo, permitiendo la interacción con el usuario final.

1.7.2 MODELO TCP/IP [3-4], [8], [11-12], [31], [55]

El modelo TCP/IP es más que un modelo de referencia, este es el estándar de red utilizado en la actualidad; emplea la misma lógica que OSI al manejar su estructura por niveles, sin embargo define de una forma diferente los niveles del modelo como se puede observar a continuación:

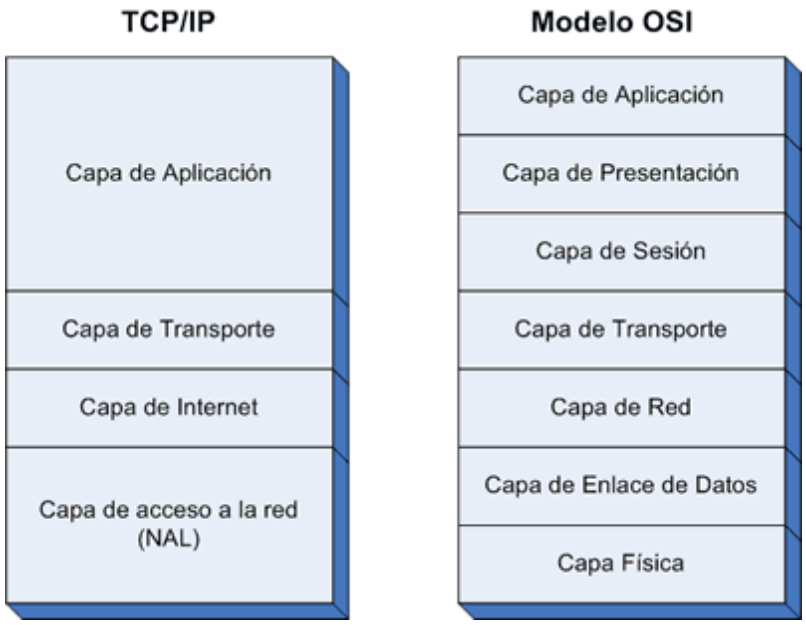


Figura 22. Comparación de modelos de red [52]

Dentro del modelo TCP/IP se definen cuatro capas: capa de acceso, internet, transporte y aplicación. La capa de acceso contiene la capa física y enlace de datos dentro de su correspondiente modelo OSI, en la cual se establece tanto la transmisión de la señal por el medio físico, los procedimientos y características mecánicas y eléctricas para la transmisión de los bits por medio del canal físico, además de su direccionamiento dentro de las capas MAC y LLC; la capa Internet en cambio se encarga de realizar el direccionamiento lógico de la red efectuando el enrutamiento de los paquetes, además de ser la responsable de los procedimientos de inicio y fin de transmisión, así como los procedimientos de conmutación, definiendo los protocolos ICMP[24], IP[25], ARP[26], RARP[27], entre otros.

Dentro de la capa de transporte se realiza una conexión de extremo a extremo conociéndose también como conexión entre host ya que solo los sistemas finales se comunican a este nivel, además dentro de esta capa se deben segmentar los datos generados por la capa aplicación en segmentos más pequeños facilitando de esta manera su trasportación; así mismo, estos datos pueden transmitirse en una forma fiable o no fiable dependiendo del protocolo a utilizarse.

[24] ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
[25] IP: Internet Protocol (Protocolo de Internet)
[26] ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)
[27] RARP: Reverse Address Resolution Protocol (Protocolo de Resolución de Dirección Inversa)

Si se utiliza un protocolo TCP[28] u orientado a conexión, se trata de un protocolo fiable ya que se asegura que los datos sean transmitidos correctamente, además se asegura que los mismos lleguen a su destino, así también se maneja control de flujo, control de congestión y secuenciamiento de mensajes. Al contrario si se utiliza un protocolo UDP[29] o no orientado a conexión, se trata de un tipo de transmisión basada en el principio del mejor esfuerzo, es decir que una vez que los datos fueron enviados no se asegura que los mismos lleguen sin errores o lo que es más que éstos lleguen a su destino; útil para el transporte de los mensajes en el menor tiempo posible.

En la capa de aplicación se trabaja con protocolos que trabajan a nivel aplicación dentro de los cuales se tienen varios protocolos como HTTP[30], HTTPS[31], FTP[32], TELNET[33], POP[34], POP3, IMAP[35], SSH[36], SMTP[37], entre otros.

TCP/IP es un protocolo utilizado por todas las redes actuales para su comunicación entre sí, este modelo fue concebido para que trabaje bajo cualquier sistema operativo y cualquier tipo de software independientemente de la tecnología de transmisión que se utilice y bajo cualquier red física.

1.7.2.1 Direccionamiento en TCP/IP v4

Las direcciones de capa de red o direcciones lógicas se encuentran contenidas en esta capa y está conformada por 32 bits dividida en cuatro octetos.

Las clases de direcciones IPv4 se dividen en cinco: las Clases A, B, C, D y E, utilizadas cada una dependiendo del tamaño de la red. La definición de clases se realiza en base al primer octeto como se muestra a continuación:

[28] TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)
[29] UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario)
[30] HTTP:Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)
[31] HTTPS: Hypertext Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)
[32] FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)
[33] TELNET: Telecomunicación Network (Red de Telecomunicaciones)
[34] POP: Post Office Protocol (Protocolo de la oficina de correo)
[35] IMAP: Internet Message Access Protocol (Protocolo de Acceso a Mensajes Internet)
[36] SSH: Secure Shell (Intérprete de Comandos Seguro)
[37] SMTP: Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)

Tabla 1. Definición de clases - Direccionamiento IPv4 [57]

Primer Octeto	Clase de dirección
1 – 126	Clase A
128 – 191	Clase B
192 – 223	Clase C
224 – 239	Clase D
240 – 255	Clase E

De las cinco clases de direcciones de red, las tres primeras son las que se utilizan para identificar equipos en la red, distinguiéndose por la densidad de direccionamiento que provee cada una de ellas como se indica más adelante. La clase D son direcciones de multidifusión, algunas de estas son utilizadas por los protocolos de enrutamiento OSPF[38], EIGRP[39] o RIPv2[40]; en cambio las direcciones de clase E son utilizadas solo para fines experimentales.

1.7.2.1.1Estructura de una dirección IP

Una dirección IP consta de dos partes, la parte de red y la parte de host. Para diferenciar la parte de red de la parte de host se utiliza la máscara de red.

Las máscaras de red por defecto en función de su clase son las siguientes:

Tabla 2. Definición de máscara de red en función de la clase [3]

Clase de dirección	Máscara de Red(decimal)	Máscara de Red(binario)
Clase A	255.0.0.0	11111111.00000000.00000000.00000000
Clase B	255.255.0.0	11111111.11111111.00000000.00000000
Clase C	255.255.255.0	11111111.11111111.11111111.00000000

En un formato binario los “1” representan la parte de red y los “0” representan la parte de host.

[38] OSPF: Open Shortest Path First (Primero el camino libre más corto)
[39] EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de enrutamiento de gateway interior mejorado).
[40] RIP: Routing Information Protocol (Protocolo de información de enrutamiento).

El número de host se determina mediante la aplicación de la fórmula de 2^n-2, de igual forma se aplica la misma fórmula para el cálculo del número de redes. En la siguiente tabla se muestra el número de redes y de host para las direcciones clase A, B y C.

Tabla 3. Número de redes y host en función de la clase [3]

Clase de dirección	Número de Redes	Número de host por red
Clase A	126	16777214
Clase B	16384	65534
Clase C	2097152	254

Aunque existe un amplio rango de direcciones de red, el crecimiento de las mismas ha causado un agotamiento de las direcciones IP públicas, es decir de las direcciones que permiten identificar los dispositivos conectados en la red global o pública, por lo cual se ha designado un rango de direcciones IP para un direccionamiento privado, el mismo que puede ser utilizado repetidamente en cada institución. El rango de direcciones asignadas se puede ver en la siguiente tabla.

Tabla 4. Rangos de direccionamiento IP privado [57]

Rango de direcciones privadas[57]
10.0.0.0 a 10.255.255.255
172.16.0.0 a 172.31.255.255
192.168.0.0 a 192.168.255.255

Las clases realizan una subdivisión de redes muy rígida, con un tamaño mínimo de 255 host, provocando un desperdicio de muchas direcciones IP por lo que se hizo necesario desarrollar nuevos procedimientos enfocados a optimizar su uso, como subnetting y vlsm.

1.7.2.2 Subnetting

El subnetting implica dividir direcciones full class en pequeñas subredes, lo cual permite tener una mejor organización de las redes grandes además de permitir contar con subredes adicionales sin la necesidad de ocupar más direcciones IP,

con esto también se logra reducir los dominios de broadcast en la red. Al aplicar subnetting en una red se quita el concepto de clases de direcciones de red y se habla de direcciones sin clase o classless, de esta manera se facilita la administración y diseño de la red.

El hecho de aplicar subnetting en una red implica el coger prestado bits de la parte de host para crear nuevas subredes. Para realizar este procedimiento basta con aplicar la fórmula:

- Número de host por subred = 2^n-2
- Número de subredes = 2^n-2

  donde n indica el número de bits utilizados.

Es necesario restar 2 debido a que en cada subred creada se tiene una dirección de red y una dirección de broadcast.

Para ilustrar mejor este concepto se puede revisar el siguiente ejemplo donde una red Clase C puede ser subneteada en base al número de bits prestados obteniéndose las siguientes máscaras de red.

Tabla 5. Ejemplo de subnetting en una red clase C

Número de bits prestados (n)	Máscara de subred (Notación Decimal)	Máscara de subred (Notación Binaria)
0	255.255.255.0	11111111.11111111.11111111.00000000
1	255.255.255.128	11111111.11111111.11111111.10000000
2	255.255.255.192	11111111.11111111.11111111.11000000
3	255.255.255.224	11111111.11111111.11111111.11100000
4	255.255.255.240	11111111.11111111.11111111.11110000
5	255.255.255.248	11111111.11111111.11111111.11111000
6	255.255.255.252	11111111.11111111.11111111.11111100

Es necesario tener en cuenta que a mayor cantidad de subredes se tiene una menor cantidad de host y viceversa.

El subnetting aunque para muchas de las aplicaciones puede resultar conveniente; este procedimiento no es eficiente, ya que todas las subredes que

se crean a partir de la original tendrán la misma máscara de red, por lo cual es necesario revisar el concepto de VLSM[41].

1.7.2.3 VLSM ó Variable Length Subnet Mask (Máscara de Subred de Longitud Variable.)

VLSM permite incluir más de una máscara de subred en una red, permitiendo optimizar la asignación de direcciones IP, además ofrece una mayor capacidad de utilizar la sumarización de rutas. Con VLSM además es posible subdividir a una subred, utilizando subredes de diferentes tamaños según la necesidad.

Al aplicar VLSM a una red ya no se tendrán necesariamente subredes con una máscara de red fija sino mas bien las máscaras de subredes creadas tendrán su propia máscara ajustándose a los requerimientos de la red. Para el cálculo de las nuevas subredes al igual que en subnetting se aplica la regla de 2^n-2, (donde n=número de bits prestados), en donde los bits asignados para la parte de red definen también su máscara a partir de la cual se determina la parte para host asignada.

Al aplicar un direccionamiento eficiente o subnetting en las redes, desaparece el concepto de clases ya que las máscaras son variables.

1.7.3 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento utilizan algoritmos que indican la puerta de salida para los diferentes paquetes de datos. A nivel interno los ruteadores, equipos de la capa de red, realizan dos procesos:

- manejar los paquetes en función de su llegada buscando en las tablas de enrutamiento la puerta de salida del mismo y,
- llenar y actualizar las tablas de enrutamiento.

Los protocolos de enrutamiento pueden ser del tipo estático o dinámico; los protocolos de enrutamiento dinámico se subdividen en función del algoritmo utilizado, por vector distancia o estado de enlace.

[41] VLSM: Variable Length Subnet Mask (Máscara de Subred de Longitud Variable)

1.7.2.4.1 Enrutamiento Estático

Toda la información se almacena de manera estática en el ruteador, por lo cual cada actualización que se necesite debe realizarse de manera manual, además se debe asegurar que cada uno de los enrutadores contengan las rutas adecuadas, de manera que se pueda intercambiar tráfico.

1.7.2.4.2 Enrutamiento dinámico

La información es compartida de manera dinámica por los ruteadores; la actualización de las tablas de enrutamiento es automática y permite identificar los cambios de topología en la red. Estos protocolos de enrutamiento permiten determinar la mejor ruta de entrega a un destino dado, en función del algoritmo utilizado.

Vector distancia: conocido como algoritmo de Bellman-Ford o Ford-Fulkerson, cada router mantiene una tabla que especifica la distancia mínima conocida hacia cada destino y la línea de salida que debe utilizarse para alcanzarlo. Las tablas son actualizadas periódicamente con la información que se obtienen de los ruteadores vecinos, estos protocolos envían copias periódicas de las tablas de enrutamiento a sus vecinos, enviando información sobre los cambios de topología. En base a la información recibida de los vecinos cada router recalcula de manera continua su tabla de distancias.

Estado de enlace: conocido como algoritmo de Dijkstra, aplica el algoritmo SPF[42] (primero la ruta más corta) manejando una base de datos completa con la información de la topología de red, ésta es utilizada para determinar la mejor ruta para un destino.

Cada router conoce las redes conectadas directamente, con lo cual crea su propio paquete de estado de enlace, que incluye la información sobre los vecinos como ID de red, tipo de enlace y ancho de banda; estos paquetes son enviados al inicio de un router, inicio del proceso de enrutamiento, o cuando existen cambios de topología.

[42] SPF: Shortest Path First (Primero la Ruta más Corta)

Protocolos basados en vector distancia.

RIP: Protocolo de Enrutamiento Interior por vector distancia. Utiliza como métrica el conteo de saltos, máximo 15. Envía actualizaciones cada 30 segundos. La mejor ruta es elegida en función de la menor cantidad de saltos hacia el destino dado.

IGRP[43]**:** Protocolo de Ruteo de Gateway Interior, propietario de Cisco. Su métrica está basada en el ancho de banda, carga, retardo y confiabilidad. Las actualizaciones son enviadas cada 90 segundos. La mejor ruta es elegida en función de la métrica calculada a partir de los parámetros medidos.

EIGRP: Protocolo mejorado de Enrutamiento de Gateway Interior por vector distancia, propietario de Cisco. Su métrica está basada en el ancho de banda, carga, retardo y confiabilidad. Utiliza el algoritmo de actualización DUAL para calcular la ruta más corta, no envía actualizaciones automáticas, éstas son dadas para informar cambios de topología y enviar la información solo a los routers que necesitan la información. EIGRP utiliza una tabla de topología independiente de la tabla de enrutamiento, la misma que incluye la mejor ruta y rutas de respaldo sin lazos.

BGP[44]**:** Protocolo de enrutamiento exterior de vector distancia utilizado para la comunicación interdominio e intradominio. La información intercambiada incluye el camino dentro del sistema autónomo que deben seguir los paquetes para alcanzar una red determinada. La información de las tablas de rutas es intercambiada entre los router extremos de un sistema autónomo. Para delimitar y configurar la información que se intercambia en el protocolo BGP es necesario crear sistemas autónomos, de manera que cada uno de ellos cuente con sesiones internas (iBGP) y externas (eBGP).

BGP intercambia información sobre el encaminamiento entres sistemas autónomos que garantiza la elección de rutas sin bucles; para la definición de las métricas se basa en políticas de red o reglas de los atributos BGP.

[43] IGRP: Interior Gateway Routing Protocol (Protocolo de Ruteo de Gateway Interior)
[44] BGP: Border Gateway Protocol (Protocolo de Gateway de Borde)

Protocolos basados en estado de enlace.

OSPF: Es un protocolo de Enrutamiento Interior de estado de enlace (Open Shortest Path First) que permite dividir un sistema autónomo en unidades jerárquicas de menor tamaño, enlazándolas con un área de backbone. Las publicaciones del estado de enlace son enviadas a los miembros de una misma unidad jerárquica. Este protocolo calcula la distancia más corta entre un nodo origen y el destino al determinar la ruta en función de la métrica obtenida, estas métricas están dadas en base a una serie de parámetros como el rendimiento, retardo, costo y fiabilidad. Las actualizaciones de topología son enviadas en base a los cambios que ocurran en la misma, los routers realizan publicaciones de estado de enlace con información de los vecinos y los costos de las rutas, con el objetivo de mantener actualizada la base de datos.

Además OSPF cuenta con una base topológica representada mediante un grafo, la misma que es manejada por cada dispositivo de enrutamiento.

IS-IS[45]**:** Sistema Intermedio - Sistema Intermedio (Intermediate System - Intermediate System) adoptado por la ISO para utilizarlo con el protocolo de capa de red sin conexiones CNLP[46]. IS-IS forma una base topológica a partir de la cual se calculan las rutas más cortas para alcanzar un destino. La información de cada router es enviada por medio de paquetes LSP[47] (Link State PDU) dentro de los cuales se indica el estado de los enlaces y las direcciones de capa de red que se pueden alcanzar de manera directa.

En su mayor parte las innovaciones de IS-IS fueron acogidas por el protocolo OSPF que fue creado unos años más tarde, por lo cual no existen mayores diferencias entre los dos tipos de protocolos a excepción del manejo de información simultánea de varios protocolos de capa de red, la cual es una característica propia de IS-IS.

[45] IS-IS: Intermediate System - Intermediate System (Sistema Intermedio - Sistema Intermedio)
[46] CNLP: Connectionless Network Layer Protocol (Protocolo de capa de red sin conexión)
[47] LSP: Link State PDU (PDU de estado de enlace)

1.8 FUNDAMENTOS DE CONSTRUCCIÓN DE UNA RED LAN

1.8.1 INTRODUCCIÓN

Un sistema de cableado estructurado es una de las partes fundamentales de cualquier edificación, ya que soporta aplicaciones como voz, video y datos, constituyéndose en la base para la operación de todos los sistemas, al ser una de las partes vitales de la red.

Es importante tener en cuenta que los sistemas de cableado estructurado tienen una duración aproximada de 15 años por lo que su diseño debe permitir y facilitar futuros cambios o ampliaciones en la red, teniendo en cuenta una debida planificación de crecimiento sobre la red actual.

1.8.2 ANTECEDENTES

En sus inicios los edificios eran construidos tomando en cuenta dos servicios básicos, telefonía y red de datos. Sin embargo al no contar con estándares para su uso e instalación, los proveedores de equipamiento realizaban instalaciones de cable de acuerdo a sus necesidades, lo cual dificultaba en gran manera el cambio de proveedor para los clientes, ya que si se utilizaba nuevo equipamiento éste necesitaba de otras conexiones de red, obligándole al cliente a continuar con el antiguo proveedor o gastar grandes cantidades de dinero para realizar una nueva instalación de cable.

Además las conexiones de red realizadas no brindaron flexibilidad ya que no se adaptaban a los cambios en una organización, así también si se necesita añadir un servicio a la red era necesario añadir una nueva conexión de red, y hacer esto cada vez que se necesite añadir servicios a la misma.

En base a estas complicaciones que se presentaron tanto para proveedores como clientes, se hace necesario la creación de estándares que garanticen el funcionamiento de la red independientemente del proveedor, brindando compatibilidad entre los productos y que además se ajuste a los requerimientos de red y soporten las aplicaciones actuales y futuras en una red teniendo en cuenta un período de al menos 10 años.

1.8.3 CARACTERÍSTICAS DE UN SISTEMA DE CE[48]

Un sistema de cableado estructurado se caracteriza por:

Administración centralizada.- permite realizar una fácil localización de daños o averías y una rápida corrección de daños sin que la red quede completamente fuera de servicio.

Flexibilidad.- debido al cambio constante de los ambientes de trabajo un sistema de CE permite configurar nuevos puestos de trabajo, modificando solo el enlace deseado.

Reducción de costos de instalación y mantenimiento.- debido a que su administración e instalación se realiza en un entorno centralizado se reducen los costos en la instalación, así también su mantenimiento se simplifica.

Solución segura: al contar con cuartos de telecomunicaciones se protege el corazón de la red, al resguardarlo de accesos no autorizados, pero además se brinda el acceso y facilidad de conexión de las estaciones de trabajo hacia las tomas de comunicaciones.

Todo sistema de cableado estructurado se basa en normas y estándares que facilitan la administración detección y resolución de problemas de comunicaciones debido a que estas normas brindan los lineamientos para su instalación y administración.

1.8.4 ORGANIZACIONES DE ESTANDARIZACIÓN [41], [43], [56], [58-61]

ISO.- La Organización Internacional de Estándares (*International Standards Organization*) es una organización no gubernamental cuya función se centra en el desarrollo y publicación de estándares de calidad con la finalidad de facilitar el comercio a nivel mundial en lo relacionado a bienes y servicios, desarrollo científico, intelectual, tecnológico y económico.

Para la aceptación de un estándar se realiza un proceso que garantiza su aceptación.

[48] CE: Cableado Estructurado

IEEE.- El instituto de Ingenieros Eléctricos y Electrónicos (The Institute of Electrical and Electronics Engineers) es una sociedad que desarrolla estándares para las industrias eléctricas y electrónicas, particularmente en el área de redes de datos.

El IEEE promueve la creatividad, el desarrollo y la integración, además de compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general.

ANSI: El Instituto Nacional Americano de Normalización (American National Standards Institute) es una organización privada sin fines lucrativos que administra y coordina la normalización voluntaria y las actividades relacionadas a la evaluación de conformidad en los Estados Unidos. Su principal objetivo es mejorar tanto la competitividad mundial de las empresas estadounidenses, así como la calidad de vida de los mismos, promoviendo y facilitando normas voluntarias de consenso y sistemas de evaluación de conformidad y protegiendo su integridad.

EIA: La Alianza de Industrias Electrónicas (Electronic Industries Alliance) es una organización comercial acreditada por la ANSI que desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, información electrónica, telecomunicaciones y seguridad de internet.

TIA: La Asociación de Industrias de Telecomunicaciones (Telecommunications Industry Association) es una asociación comercial global con sede en los Estados Unidos que representa alrededor de 600 empresas de telecomunicaciones, acreditada por la ANSI para el desarrollo de normas voluntarias de la industria para una amplia variedad de productos de telecomunicaciones. *"Dentro de TIA representantes de fabricantes, proveedores de servicios y usuarios finales, incluyendo el gobierno forman parte de la formulación de los grupos involucrados en el establecimiento de normas"*. [61]

1.8.5 NORMAS Y ESTÁNDARES DE CE VIGENTES [13-16]

Todo sistema de cableado estructurado se rige en base a lineamientos para su buen funcionamiento, dentro de las normas de cableado estructurado están:

ANSI/TIA/EIA-568-B: Estándar de cableado de telecomunicaciones para edificios comerciales.

- *TIA/EIA-568-B.1: Requerimientos generales.*

Especifica criterios básicos para que un sistema de cableado estructurado brinde funcionalidad ante multi-productos y multi-vendedor, mediante la planificación e instalación de un sistema estructural de cableado.

Este estándar además establece los criterios técnicos de configuración de un sistema de cableado estructurado, el acceso y conectorización de los elementos, estudiando cada uno de los componentes de un SCE[49], requerimientos de instalación y los test necesarios para su buen funcionamiento.

- *TIA/EIA-568-B.2: Componentes de cableado par trenzado balanceado.*

El rendimiento de una transmisión depende principalmente de las características del cableado horizontal, conectores utilizados, patch cords empleados, los cuidados que se tengan durante su instalación y el mantenimiento que se brinde al mismo, este estándar trata sobre los elementos que intervienen en la instalación del cableado par trenzado para que cumpla con los parámetros mínimos para una transmisión y buen rendimiento teniendo en cuenta los criterios que se establecen para su funcionamiento.

- *TIA/EIA-568-B.3: Estándar de componentes de cableado de fibra óptica.*

El estándar especifica los componentes y requerimientos de transmisión en un sistema de cableado de fibra óptica tanto multimodo como monomodo y los cables reconocidos, estudiando la conectorización del hardware, patch cords, e instrumentos de verificación.

[49] SCE: Sistema de Cableado Estructurado.

ANSI/TIA/EIA-569: Estándar de recorridos y espacios en edificios comerciales de telecomunicaciones.

En este estándar se reconocen tres conceptos básicos:

Los edificios son dinámicos, en el transcurso de su vida útil se producen continuas remodelaciones del espacio, constituyéndose esto en una regla.

Tanto los medios de transmisión como los equipos de telecomunicaciones cambian dramáticamente, independientemente de su fabricante.

Las telecomunicaciones implican más que voz y datos, se incluyen además sistemas de control, seguridad, audio, televisión, sensores, alarmas e intercomunicadores, inclusive servicios inalámbricos y también la trasmisión de datos por medio de cables del sistema eléctrico.

Es muy importante considerar que para que un edificio se adapte al sistema de telecomunicaciones su diseño debe incorporarse en la etapa de diseño arquitectónico, incluyéndose los diseños de rutas y espacios de telecomunicaciones que puedan adaptarse a las futuras necesidades de sus ocupantes.

ANSI/TIA/EIA-606-A: Estándar de administración de infraestructuras de telecomunicaciones comerciales.

El estándar provee una guía para la administración y el mantenimiento de la infraestructura de telecomunicaciones. Su administración se la divide por clases; la clase 1 es para edificios simples, los cuales brindan servicio desde un único cuarto de equipos; la clase 2 se la utiliza para edificios sencillos que tienen un cuarto de equipos y varios cuartos de telecomunicaciones; la clase 3 es utilizada para campus con varios edificios interconectados y la clase 4 es para ambientes multicampus.

Además el estándar establece la identificación de cada uno de los componentes y subsistemas basados en colores, códigos y etiquetas los cuales permitan identificar fácilmente cada uno de los servicios implementados.

ANSI/TIA/EIA-J-STD-607-A: Requerimientos de puesta a tierra para la infraestructura de telecomunicaciones en edificios comerciales.

Esta norma especifica como debe realizarse la conexión del sistema de tierras, frecuentemente un sistema de puesta a tierra es diseñado e instalado luego que el edificio ha sido construido y equipado. Su diseño debe soportar una infraestructura independiente del vendedor y de los productos empleados. Además es importante considerar que las infraestructuras actuales deben soportar las múltiples aplicaciones de un sistema de cableado estructurado.

ANSI/TIA/EIA-TSB-67: Especificación para la prueba en el campo del rendimiento de transmisión de sistemas de cableado de par trenzado sin blindaje.

Mediante el boletín técnico se detalla las especificaciones y procedimientos para la validación y certificación del cableado estructurado ya instalado en una edificación. El boletín establece como marco de referencia dos tipos de configuraciones de verificación por enlace básico o canal; estos dos tipos de configuraciones se diferencian básicamente por los componentes que incluyen su configuración, en el caso del canal se abarca tanto el enlace permanente como los patch cord de conexión utilizados en el ambiente de trabajo, en cambio en el caso del enlace no se consideran los patch cord sino más bien enlaces de prueba.

Los parámetros que se analizan en la certificación del cableado estructurado son los siguientes:

- **Mapa de Cableado:** realiza una verificación de las terminaciones pin a pin, además de verificar errores de conectividad en las instalaciones.

  Por cada uno de los conductores el mapa de cableado indica.

  - Continuidad con el extremo remoto.
  - Pares reversos
  - Pares divididos
  - Pares transpuestos
  - Cualquier otro defecto de conexión.

Su correcta conectividad está basada en la norma ANSI/TIA/EIA-568-B.2

- **Longitud:** la longitud física del enlace está defina por la suma de los enlaces independientes existentes entre dos puntos finales. La longitud máxima de un enlace permanente es de 90m.

- **Pérdida de inserción:** es medida por la pérdida de señal en un enlace permanente. Ésta se origina por la pérdida de energía eléctrica en la resistencia del cable.

  Su valor se mide en dB, para valores más bajos de atenuación se tiene un mejor rendimiento del cable.

- **Pérdida de Retorno:** se mide como la diferencia entre la potencia de la señal transmitida y la potencia de las reflexiones de la señal causadas debido a las variaciones en la impedancia de la señal. Los valores altos indican que los cables son más eficientes para la transmisión de señales en una red LAN ya que se pierde poca señal por causa de reflexiones.
- **Pérdida de paradiafonía NEXT[50]**: ó interferencia de extremo cercano. Causada por la interferencia de señales cercanas de un par de cables en otro par cercano.

  El NEXT se expresa en dB, para valores más altos de NEXT se tiene menor interferencia en la señal y un mejor rendimiento del cable utilizado.

- **Pérdida de paradiafonía por suma de potencia (PSNEXT[51]):** es la combinación de forma estadística del crosstalk recibido de los pares desde los extremos cercanos que operan simultáneamente.

- **Pérdida de paradiafonía en el extremo lejano por igualación de nivel (ELFEXT[52]):** indica la relación entre el FEXT[53] y la atenuación. Es una medida expresada en dB, influida por el trenzado de los cables, el

[50] NEXT: Near-End crosstalk (Interferencia de Extremo Cercano - Paradiafonía)
[51] PSNEXT: Power Sum Near-End crosstalk (Paradiafonía de suma de potencias)
[52] ELFEXT: The Equal-Level Far-End Crosstalk (Telediafonía por igualación de nivel)
[53] FEXT: Far-End Crosstalk (Interferencia de Extremo Lejano - Telediafonía)

apantallamiento, así también la frecuencia de trabajo y la longitud del enlace. Un nivel alto de ELFEXT indica una buena transmisión del enlace.

- **Pérdida de paradiafonía en el extremo lejano por igualación de nivel y suma de potencia (PSELFEXT[54]):** es una medida que se deriva del cálculo de las medianas del ELFEXT de cada par de cables. Su medida se encuentra influenciada por el trenzado de los cables, su apantallamiento, además de la frecuencia de trabajo y la longitud del enlace. Un valor alto de esta medida está relacionado a una buena transmisión en el enlace.

- **Retardo en la propagación:** indica el tiempo en que una señal tarda en propagarse de un extremo a otro.

- **ACR[55]:** indica la relación entre la atenuación y la interferencia. Un valor alto de ACR indica que las señales recibidas son mucho más grandes que la interferencia, ó que se tiene un NEXT alto y valores de atenuación bajos.

1.8.6 COMPONENTES DE UN SISTEMA DE CE

Un sistema de cableado estructurado está compuesto por varios componentes como se explica a continuación, en base a la norma ANSI/TIA/EIA-568-B.

1.8.6.1 Subsistema horizontal

El cableado horizontal es aquel que se extiende desde el cuarto de telecomunicaciones hasta la toma ubicada en el área de trabajo. Este subsistema incluye el cable horizontal, conectores, terminaciones, patch cords, puntos de consolidación y la ducteria.

Dentro de los servicios y sistemas más comunes considerados dentro del cableado horizontal están: servicios de voz de telecomunicaciones, equipamiento local de conmutación, comunicaciones de datos, redes LAN, servicios de video y otros relacionados a sistemas de señalización en construcciones.

[54] PSELFEXT: Power Sum the Equal-Level Far-End Crosstalk (Telediafonía de suma de potencias)
[55] ACR: Attenuation/Crosstalk Ratio (Relación atenuación - diafonía)

La distancia máxima permitida en un sistema de cableado horizontal es de 90m, dentro de los cables reconocidos en la norma están el cable UTP de 100 ohmios categoría 3 o superior (categoría 5e o 6 recomendada) y/o cables de dos o más fibras ópticas multimodo.

1.8.6.2 Subsistema Vertical

Su función es proporcionar la interconexión entre cuartos de telecomunicaciones, cuartos de equipos y facilitar la entrada del cableado de telecomunicaciones. Este cableado incluye cables de backbone, conexiones cruzadas principales e intermedias, mecanismos de terminación, patch cord o jumpers usados para la conexión de backbone a backbone, incluyendo además la interconexión entre edificios.

El sistema de cableado vertical o de backbone usa una topología jerárquica en estrella ya que esta permite flexibilidad y fáciles variaciones, debiendo tenerse no más de dos niveles, porque de esta manera se limita la degradación de la señal en sistemas pasivos y además simplifica los movimientos, adiciones o cambios.

Los medios de transmisión permitidos en este tipo de cableado son: Cable par trenzado multipar de 100 ohmios, cable de fibra óptica multimodo entre 62,5/125um, 50/125um o cable de fibra óptica monomodo; las distancias de cableado vertical permitidas se pueden observar en la siguiente tabla:

Tabla 6. Distancias permitidas para el cableado vertical según el medio de transmisión utilizado [13]

Tipo de Medio	Alcance
Par trenzado 100 ohmios (transmisiones de voz)	Máximo 800m
Cable multipar cat. 3 de 100 ohmios	90m a 16MHz
Cable multipar cat. 5e de 100 ohmios	90m a 100MHz
Fibra óptica de 62,5/125 um	Máximo 2000m
Fibra óptica de 50/125 um	Máximo 2000m
Fibra óptica monomodo	Máximo 3000m

1.8.6.3 Área de trabajo

El área de trabajo se ubica desde la toma de telecomunicaciones hasta el equipo del usuario. El cableado en el área de trabajo debe estar diseñado para permitir una fácil adición, modificación o cambio ya que estas tomas no necesariamente son permanentes.

Para la salida del conector de cable UTP o ScTP de cuatro pares se utilizan jack modulares de ocho posiciones, cuya asignación de pines puede definirse en base a las normas:

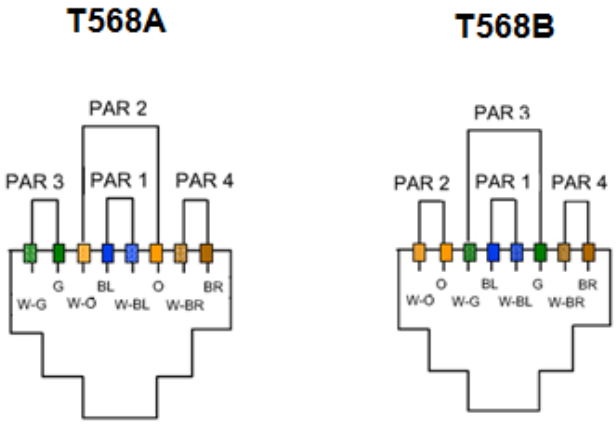


Figura 23. Asignación de pines según la norma aplicada [13]

Los cables de conexión utilizados en el área de trabajo no deben exceder los 5 metros y dependiendo de la aplicación puede ser necesario utilizar ciertos componentes como: cable especial o adaptador, adaptador en Y, adaptadores pasivos, adaptadores activos, entre otros.

Además es importante considerar que dentro de las áreas de trabajo también se debe considerar el caso del cableado en las denominadas oficinas abiertas, las cuales manejan una infraestructura modular muy susceptible a cambios, en las cuales cuando se realizan cambios se debe desechar todo el cableado retirado; sin embargo para evitar estos acontecimientos se implementan los MUTOAs (Multi-User Telecommunications Outlet Assembly) con lo cual se tiene la terminación de todos los cables horizontales en un lugar fácilmente accesible por todas las estaciones de trabajo, dando servicio a un máximo de 12 estaciones de trabajo. Los MUTOAs no deben estar instalados en pisos o techo falso ya que su ubicación será permanente.

1.8.6.4 Cuarto de Telecomunicaciones

Los cuartos de telecomunicaciones comprenden un área específica para los equipos de telecomunicaciones e incluyen las terminaciones del cableado vertical y horizontal, sistemas de seguridad, audio, televisión por cable, entre otros sistemas de telecomunicaciones. Los cuartos de telecomunicaciones no pueden contener instalaciones eléctricas que no sean propios de los sistemas de telecomunicaciones, además es necesario que los mismos cuenten con reguladores y UPS[56] ante fallas de energía. Así también en los cuartos de telecomunicaciones debe proveerse un ambiente controlado, verificando su temperatura y humedad.

1.8.6.5 Cuarto de Equipos

Un cuarto de equipos se diferencia de un cuarto de telecomunicaciones por la naturaleza y complejidad del equipamiento. Un cuarto de equipos puede brindar alguno o todos los servicios de un cuarto de telecomunicaciones. En un cuarto de equipos además se cuenta con un espacio adicional para estaciones de trabajo del personal de Administradores.
Toda edificación debe contar con al menos un cuarto de equipos o cuarto de telecomunicaciones dependiendo de la densidad de usuarios.

1.8.6.6 Cuarto de Entrada de Servicios

El cuarto de entrada de servicios abarca a todos los servicios de entrada de telecomunicaciones al edificio, incluyendo conectividad de hardware, dispositivos de protección y el equipamiento necesario para facilitar la entrada del cableado.

1.8.6.7 Sistema de Puesta a tierra

Todo sistema de cableado estructurado debe tener un sistema de puesta a tierra basado en el estándar ANSI/EIA/TIA-607.

[56] UPS: Uninterruptible Power Supply (Fuente de Alimentación Ininterrumpible)

1.8.7 TIPOS DE ETIQUETADO

En base a la norma EIA/TIA-606 de acuerdo a la etiquetación se especifica que tanto el tamaño, como el color y el contraste deben ser seleccionados cuidadosamente de modo que la identificación sea fácilmente leída. El etiquetado realizado debe ser visible durante la instalación y el mantenimiento.
Además para facilitar su identificación se ha especificado un color según el tipo de terminación como se puede observar en la siguiente tabla:

Tabla 7. Asignación del color según el tipo de terminación [15]

Tipo de Terminación	Color
Punto de demarcación	Naranja
Conexión de red	Verde
Equipamiento	Purpura
Sistema Clave	Rojo
Primer nivel de Backbone	Blanco
Segundo nivel de Backbone	Gris
Backbone entre edificios	Café
Horizontal	Azul
Otros (alarmas sistemas de seguridad,..)	Amarillo

Su etiqueta debe permitir una fácil identificación de los componentes del sistema de cableado estructurado así como su ubicación por lo cual es muy importante que el diseño de su inscripción sea tratado cuidadosamente.

CAPITULO 2. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS DE UN ENTE DEL MINISTERIO DE DEFENSA NACIONAL

2.1 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.

Dentro de 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.

Mediante la realización del levantamiento y análisis de información de la situación actual de red, con su topología y elementos constituyentes es posible tener una idea clara de su estado actual, para lo cual se debe tener en cuenta 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.

2.2 LEVANTAMIENTO DE INFORMACIÓN

Las instalaciones de la institución tienen aproximadamente un uso de 10 años a partir de su construcción. A lo largo de su vida útil la edificación ha sufrido cambios a nivel internos afectando esto a su estructura de red; así también la masificación del uso de las TIC[57] ha obligado a la infraestructura de red presente a adaptarse a los requerimientos, demandando nuevos puntos de red para la prestación del servicio.

Sin embargo debido a que en sus inicios no se consideró tal crecimiento ni el uso masivo de nuevas tecnologías de información, hace necesario que se realice un estudio que permita identificar el estado actual de la red y sus requerimientos en cuanto a servicios y seguridad de la misma. Para esto es necesario comenzar con un levantamiento de información, el cual muestre las características propias de la red y brinde una idea clara de su estructura, teniendo en cuenta además que al momento no existe documentación actualizada de la misma.

2.2.1 CABLEADO ESTRUCTURADO

El cableado estructurado de cualquier institución constituye la base fundamental para la prestación de servicios de red, por lo cual es importante que este se encuentre en perfecto estado.

Dentro del levantamiento de información del cableado estructurado se han considerado 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.

2.2.1.1 Subsistema Horizontal

- El cableado horizontal del edificio es par trenzado categoría 5e, para su distribución cada uno de los bloques del edificio cuentan con su respectivo cuarto de telecomunicaciones y bandejas metálicas de distribución.
- Desde las bandejas de distribución metálicas del cableado horizontal hacia las localizaciones de salida del cableado estructurado se utiliza tubo

[57] TIC: Tecnologías de la Información y Comunicación

conduit, el cual no soporta nuevas conexiones. Las canalizaciones no sobrepasan los 6 metros en su trayectoria.

- Los conectores, terminaciones y patch cord utilizados son cable UTP categoría 5e.
- En algunos casos para la salida de los puntos de red se utiliza los ductos del interior de los modulares.
- En el rack de comunicaciones del Bloque 4 se encuentran instalados jack flotantes utilizados para reflejar algunos de los puntos de red en patch panel.
- Debido a la demanda de puntos de red se han realizado nuevas instalaciones de cableado par trenzado categoría 6a.

2.2.1.1.1 Certificación de puntos de red

La infraestructura de cableado estructurado actual con la que cuenta el edificio del Ministerio de Defensa tiene un tiempo de uso aproximado de 10 años, por lo cual, es necesario realizar la certificación del cableado estructurado con el equipamiento adecuado de todos los puntos de red, para conocer su estado y rendimiento.

Para la certificación se utilizó los equipos certificadores de red Fluke Network con los cuales se determinó el cumplimiento o no de los parámetros de red, permitiendo así determinar también el cumplimiento de las normas y estándares de cableado estructurado basados en el TSB[58] 67. *Ver 1.8.5 Normas y Estándares de CE vigentes*.

Los parámetros a considerar para la certificación del cableado estructurado del edificio se basan en el boletín técnico TSB 67, los mismos que se detallan a continuación:

- Mapa de Cableado
- Longitud del Cableado
- Pérdida de inserción
- Pérdida de Retorno

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

- Pérdida de Paradiafonía NEXT
- Pérdida de Paradiafonía por Suma de Potencia (PSNEXT)
- Pérdida de Paradiafonía en el Extremo Lejano por Igualación de Nivel (ELFEXT)
- Pérdida de Paradiafonía en el Extremo Lejano por Igualación de Nivel y Suma de Potencia (PSELFEXT)
- Retardo en la Propagación
- ACR

La certificación de los puntos de red se pueden resumir en "**Pasa**" o "**No Pasa**", para que los puntos de red pasen la certificación deben cumplir con todos los valores mínimos de los diferentes parámetros medidos. Si uno o más parámetros no cumplen con los valores umbrales mínimos definidos para cada valor, el punto de red no pasará la prueba realizada.

Los resultados de las pruebas realizadas se tratan dentro del análisis de información recopilada durante este proceso.

Las pruebas de certificación de red efectuadas a cada uno de los puntos de red del edificio, se detallan en el Anexo 3 "*Pruebas de Certificacion*".

Principales características del equipamiento utilizado.

DTX-1800 Cable Analyzer Fluke Network [62]

El DTX Cable Analyzer Series de Fluke Network es una plataforma de certificación para cableado de redes, dentro de sus principales características están:

- Tiempo de comprobación automática menor a 9 segundos.
- Ancho de Banda máximo de 900MHz.
- Almacenamiento de datos gráficos de los resultados.
- Interfaces USB /Serie.
- Adaptador de enlace permanente.
- Adaptador de canal.
- Integración de módulos de fibra óptica.
- Intercomunicación entre unidades principal y remota.

Figura 24. Características Fluke Network DTX-1800 [62]

Linkware – Fluke Network [63]

Sofware para gestión de pruebas de cableado. Permite gestionar y elaborar informes de los datos de las certificaciones de la infraestructura de cableado estructurado. Con la ayuda del software se permite descargar las pruebas realizadas y emitir los informes de las mismas. La versión utilizada es 1.4.

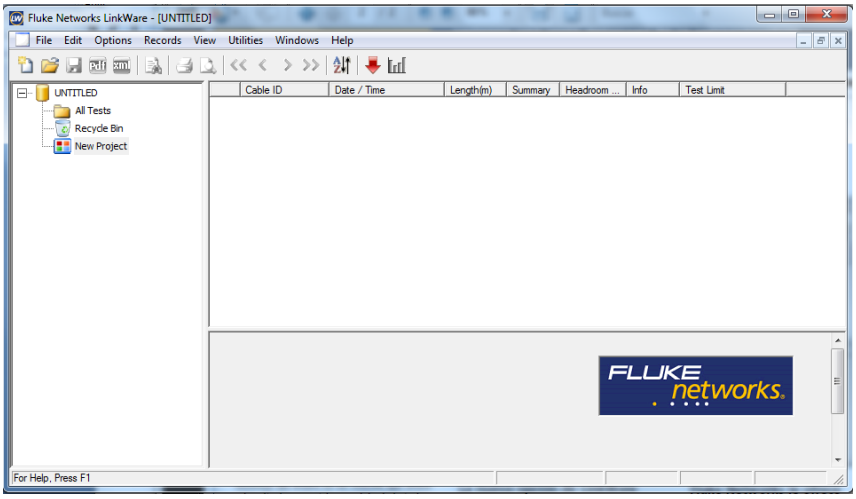


Figura 25. Software LinkWare - Fluke Network

Fuente: Software LinkWare versión 6.2

2.2.1.2 Subsistema Vertical

- El cableado vertical del edificio se encuentra conectado a través de fibra óptica multimodo FC, excepto dos de los bloques del edificio y el enlace utilizado para la conexión hacia el switch de la red wireless, los cuales se encuentran conectados con cable par trenzado UTP categoría 5e.
- Los enlaces de fibra óptica se encuentran instalados utilizando las escalerillas verticales ubicadas en los ductos de los cuartos de telecomunicaciones; de igual manera se encuentran instalados los enlaces de cable UTP.
- Los enlaces de fibra óptica no cuentan con ningún tipo de protección a lo largo de su recorrido.

2.2.1.3 Área de trabajo

- Las tomas utilizadas como salidas en las áreas de trabajo para conexión del equipo de usuario hacia la toma de conectorización, son salidas dobles que utilizan jack modulares Cat 5e.
- La asignación de los pines de los jack modulares se han definido como base en la norma T568B.
- Algunas de las tomas destinadas para el servicio de voz han sido utilizadas para el servicio de datos y viceversa.

2.2.1.4 Cuartos de Telecomunicaciones

- Cada uno de los bloques cuentan con un Cuarto de Telecomunicaciones, en los cuales se tienen Racks tipo gabinete que contienen el equipamiento de red.
- Cada rack cuenta con patch panels de datos y de voz, además de ODFs[59] para la conectorización del backbone de Fibra Óptica y switches de acceso marca 3Com serie 5500. Así también, en el rack del Bloque 4 se cuenta con un switch marca 3Com Wireless LAN Controller, al cual se conecta un Access Point marca 3Com para dar servicio a la red Wireless.
- Hacia los cuartos de telecomunicaciones llegan ductos pertenecientes al sistema de ventilación del edificio.
- Dentro de los cuartos de telecomunicaciones se encuentran instaladas cajas eléctricas de tensión para la alimentación de los sistemas de seguridad.
- Por los cuartos de telecomunicaciones pasan ductos pertenecientes a las Tuberías de Desagüe.
- El ingreso a los cuartos de telecomunicaciones se encuentra restringido al personal de administradores de red del edificio.
- Las luminarias presentes en los cuartos de telecomunicaciones son lámparas fluorescentes.
- Al interior de los cuartos de telecomunicaciones no existen lámparas de emergencia ni indicativos de salidas de emergencia.

2.2.1.5 Data Center

- En el Data Center se encuentran cuatro racks de piso tipo gabinete los mismos que albergan tanto al equipamiento activo como los servidores de aplicaciones del edificio.

[59] ODFs: Optical Distribution Frame (Repartidores de Fibra Óptica)

Tabla 8. Lista de servidores con sus respectivas IP

SERVIDOR	IP
Servidor de Base de Datos	10.10.1.10/24 10.10.1.9/24
Servidor Sigef	10.10.1.11/24
Servidor de Inventarios	10.10.1.12/24
Servidor de Correo	10.10.1.13/24 10.10.1.16/24 10.10.1.17/24
Servidor DNS Interno-Primario	10.10.1.19/24
Servidor DNS Interno-Secundario	10.10.1.18/24
Servidor de Aplicaciones Oracle	10.10.1.8/24
Servidor de Antivirus	10.10.1.14/24
Servidor de Desarrollo 01	10.10.1.20/24
Servidor Desarrollo 02	10.10.1.23/24
Servidor BLADE-INTEL 01	10.10.1.15/24
Servidor BLADE-INTEL 02	10.10.1.25/24
Servidor BLADE-INTEL 03	10.10.1.30/24
Servidor BLADE-INTEL 04	10.10.1.35/24
Servidor Controlador de Dominio	10.10.1.21/24
Servidor DNS Interno Secundario	10.10.1.22/24
Servidor de Backup	10.10.1.32/24

Fuente: Nancy Yolanda Ramón I.

Tabla 9. Lista de equipamiento activo con su respectiva IP

Equipamiento Activo	IP
Switch 3com serie 7700	172.18.1.245/24

Fuente: Nancy Yolanda Ramón I.

- El primer rack cuenta con un patch panel de datos además de ODFs para la conectorización del backbone de Fibra Óptica; desde este rack se brinda el servicio de red para todo el edificio.
- Todos los servidores del edificio se encuentran físicamente en el Data Center contenidos a partir del segundo rack; sus enlaces de conexión llegan hacia el switch de distribución.
- Todo el equipamiento activo y servidores se encuentran conectados al sistema eléctrico regulado.
- El Data Center cuenta con un sistema de enfriamiento que controla la temperatura del mismo manteniéndola entre los 20ºC y 23ºC; además se

cuenta con conexión a UPS de 80kVA los cuales protegen a la red en caso de fallas de energía.

- Todo el backbone vertical del edificio es manejado desde el Data Center.
- El Data Center cuenta con sensores de humo para detectar posibles peligros de fuego.
- El Data Center se encuentra custodiado por el personal de seguridad del edificio, además se cuenta con mecanismos de seguridad física (tarjetas magnéticas) asegurando que solo el personal autorizado ingrese al mismo.

2.2.1.6 Sistema de Puesta a Tierra

- El edificio cuenta con un sistema de puesta a tierra tipo malla.

2.2.2 ELEMENTOS DE PARTE ACTIVA

- Entre los elementos que conforman la parte activa se tienen: equipos de red y equipos de control de acceso y seguridad:

2.2.2.1 Equipos de RED

- Dentro de los equipos de red con los que cuenta la institución se tienen equipos en funcionamiento y equipos fuera de servicio, como se enumeran a continuación:

Tabla 10. Listado del equipamiento

CANTIDAD	MARCA	SERIE	ESTADO
1	Switch 3Com	7700	OPERATIVO
10	Switch 3Com	5500	OPERATIVO
1	Access Point 3Com	2700	OPERATIVO
1	Switch 3Com-Wireless	WX1200	OPERATIVO
1	Modem ADSL	VisioNet	OPERATIVO
1	Switch	D-Link	OPERATIVO
1	Router Cisco	1700	NO OPERATIVO
1	Router Cisco	3700	NO OPERATIVO
2	Switch 3Com	5500	NO OPERATIVO

Fuente: Nancy Yolanda Ramón I.

Dentro del equipamiento activo en estado operativo detallado en la tabla 10, se puede indicar lo siguiente:

- El equipo encargado de brindar conectividad tanto para internet como para la red de datos de cada uno de los Entes del Ministerio de Defensa es un switch marca 3Com serie 5500G.
- El equipo que maneja los equipos de acceso y servidores de aplicaciones es un switch marca 3Com serie 7700, este además maneja 2 enlaces de conexión pertenecientes a los administradores de red.
- A nivel de la red interna de la institución se utilizan 9 switches marca 3Com de la serie 5500 los cuales dan servicio a toda la red cableada.
- Para el servicio de red inalámbrica se cuenta con un switch 3Com Wireless LAN Controller, al cual se encuentra conectado un Access Point marca 3Com para servicio del Bloque 4.
- El Departamento de Compras Públicas cuenta con un modem ADSL[60] por medio del cual se brinda el servicio desde el Ministerio de Finanzas, contando de esta manera con un canal dedicado para esta red.
- En dos de los bloques del edificio (Bloque 2 y Bloque 4) se ha encontrado switches conectados en cascada con el fin de suplir la demanda de puntos de red en estos bloques del edificio.

Teniendo en cuenta que la red no tiene información actualizada acerca de la disponibilidad a nivel físico del equipamiento activo, se ha realizado un levantamiento de información a nivel de puertos utilizados en los switches para determinar la cantidad de puertos usados y libres. Este levantamiento se lo amplia en el Anexo 2 "*Disponibilidad del Equipamiento Activo*".

[60] ADSL: Asymmetric Digital Subscriber Line (Línea de abonado Digital Asimétrica)

Principales características del equipamiento utilizado. [64]

Switch 3com serie 7700

Figura 26. Switch 3Com serie 7700

Dentro de las principales características del switch marca 3com serie 7700 están:

- Soporte de Switching 10-Gigabit, Gigabit, y Fast Ethernet, multicapa y de alto rendimiento.
- Soporte de capa 2: Direcciones MAC[61] de 32K, 4096 VLANs, STP[62], RSTP[63] y MSTP[64].
- Soporte de capa 3: Entradas de routing IP de 64k, OSPF, RIPv1/v2, PIM SM/DM[65], IPX[66].
- Soporte de PoE.
- Plataforma de chasis integrada.
- Rendimiento de 96 Gbps.
- Ancho de banda de 240 Gbps con rendimiento del sistema de 179 Mpps.
- Capacidad de backplane de hasta 96 Gbps.
- Soporte de switching local en módulos.
- Soporte de tramas jumbo (hasta 9KB).
- Soporta módulos 10Gigabit IEEE 802.3ae para conexiones de alta velocidad entre switches.
- Soporte de login de Red.

[61] MAC: Media Access Control (Control de Acceso al Medio)
[62] STP: Spanning Tree Protocol (Protocolo de Spanning Tree)
[63] RSTP: Rapid Spanning Tree Protocol (Protocolo Rápido de Spanning Tree)
[64] MSTP: Multiple Spannig Tree Protocol (Protocolo Múltiple de Spanning Tree)
[65] PIM SM/DM: Protocol Independent Multicast Sparse Mode/Dense Mode (Protocolo Multicast Independiente Modo Esparcido/Modo Denso)
[66] IPX: Internetwork Packet Exchange (Intercambio de Paquetes Interred)

- Soporte de identificación de usuarios basado en 802.1X Radius.
- Soporte de Listas de Control de Acceso.
- Soporte de clasificación de tráfico.
- Soporte de administración de ancho de banda.
- Soporte de BGP_4, IS-IS, MSTP, y SNMP v3[67].

Switch 3com serie 5500

Figura 27. Switch 3Com serie 5500

- Switches de Capa 2/3/4 Fast Ethernet y Gigabit Ethernet.
- Funcionamiento multi-capa con rutas estáticas, RIP, OSPF, y PIM-DM y PIM-SM.
- Soporte de STP, RSTP, MSTP
- Capacidad de apilamiento XRN[68], hasta 8 unidades.
- Soporte de QoS[69] y filtrado dependiente de las aplicaciones.
- Soporte de PoE[70].
- Capacidad de switching de hasta 12,8 Gbps.
- Velocidad de transmisión de hasta 9,5 Mbps
- Ancho de banda de apilamiento de 48 Gbps (96 Gbps full-duplex).
- Manejo de listas de control de acceso (ACLs).
- Autenticación basada en usuario
- Soporte de encriptación DES[71] de 56 ó 168 bits.
- Identificación de usuarios RADIUS.
- Autenticación PAP[72]/CHAP[73]/EAPoL[74] (EAP sobre LAN).

[67] SNMP: Simple Network Management Protocol(Protocolo Simple de Administración de Red)
[68] XRN: eXpandable Resilient Networking (Networking Redundante Expansible)
[69] QoS: Quality of Service (Calidad de Servicio)
[70] PoE: Power Over Ethernet (Poder sobre Ethernet)
[71] DES: Data Encryption Standard (Estándar de Cifrado de Datos)
[72] PAP: Password Authentication Protocol (Protocolo de Autenticación de Contraseña)
[73] CHAP: Challenge Handshake Authentication Protocol (Protocolo de Autenticación por Desafío Mutuo)

- Filtrado de paquetes.
- Encriptación SNMP v3.
- Soporte de login de red IEEE 802.1X.
- Soporte de autenticación, auto-iniciación de VLAN y perfiles de QoS.
- Privilegios de acceso multinivel.

Wireless LAN Switch WX1200

Figura 28. Switch 3Com WX1200

- Puertos PoE integrado 10BASE-T/100BASE-TX.
- Auto-negociación en todos los puertos.
- Soporte de MAPs[75]: hasta 12 MAPs por switch.
- Capacidad agregada de switching: Hasta 200 Mbps.
- Soporte de dirección MAC.
- Autenticación 802.1X.
- Soporte de Virtual Private Group.
- Soporte de Mobility Profile.
- Soporte de tareas de backend de generación y autenticación de claves de encriptación.

[74] EAPOL: Extensible Authentication Protocolo over LAN (Protocolo de Autenticación Ampliable sobre LAN)
[75] MAPs: Managed Access Points (Administración de Puntos de Acceso)

Wireless LAN Managed Access Point 2750

Figura 29. AP 3Com 2750

- Un puerto integrado PoE 10BASE-T/100BASE-TX compatible con 802.3af con auto-negociación.
- Interfaces con los medios: RJ-45, 802.11a, 802.11b, 802.11g, DB-9.
- Banda de frecuencia: 802.11a: 5 GHz, 802.11b/g: 2,4 GHz.
- Distancia operativa: 802.11a: hasta 50 metros para transmisión y recepción; 802.11b/g: hasta 100 metros para transmisión y recepción.
- Consumo de alimentación: 6W máximo (puerto PoE o fuente de alimentación externa).
- Seguridad: Encriptación WEP[76] de 40/64 y 104/128 bits, TKIP[77] WPA[78] y WPA2[79] (802.11i/RSN[80]), encriptación AES de 64/128 bits; soporte de SSID[81] de broadcast múltiple en el MAP; login de red IEEE 802.1X; autenticación IEEE 802.11i o RADIUS 802.1X; soporte de ACL y VLAN en el conmutador de WLAN[82].
- Requiere un conmutador o un controlador para LAN inalámbrica de 3Com para el funcionamiento de los MAPs.

2.2.2.2 Equipos de Control y Seguridad

Existen cuatro equipos para el control de acceso por huella dactilar ubicados en las puertas de ingreso al edificio. Su instalación se encuentra asignada

[76] WEP: Wired Equivalent Privacy (Privacidad Equivalente por Cable)
[77] TKIP: Temporal Key Integraty Protocol (Protocolo de Integridad de Clave Temporal)
[78] WPA: Wifi Protect Access (Acceso Inalámbrico Protegido)
[79] WAP: Wireless Application Protocol (Protocolo de Aplicaciones Inalámbricas)
[80] RSN: Robust Secure Network (Red de Seguridad Robusta)
[81] SSID: Service Set IDentifier (Identificador de Conjunto de Servicio)
[82] WLAN: Wireless Local Area Network (Redes de Área Local Inalámbricas)

físicamente al Bloque 2. En la tabla 11 se muestra la lista de los equipos con su respectivo estado:

Tabla 11. Equipos de control y seguridad

CANTIDAD	MARCA	MODELO	ESTADO
4	Fingertec	AC900	OPERATIVO

Fuente: Nancy Yolanda Ramón I.

Estos equipos se conectan directamente al switch marca 3Com serie 5500 del Bloque 2, y su conexión se realiza utilizando cable UTP Cat 5e.

La administración de los equipos se encuentra a cargo del personal del Cuarto de Control, ubicado en el Bloque 1.

Características del AC900 Fingerprint Door Access System [65]

Figura 30. AC900 Fingerprint Door Access System

- Eliminación de incidentes por fraude de asistencia.
- Recopilación de datos de registro de forma sistemática.
- Gestión de datos rápida y eficaz a través del software.
- Restricción del acceso para el personal no registrado.
- Eliminación de incidentes por tailgating.
- Seguimiento del personal en cualquier momento.
- Control de ingreso del personal con ajuste de zona horaria.
- Integración con el sistema de cerradura de la puerta de ingreso.
- Conectividad: TCP/IP, RS232 y RS485 para conectar a la PC.

2.2.3 ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL

La topología actual de red para su estudio se la divide en dos partes, una la topología externa desde la cual se provee el servicio tanto para internet como para datos hacia los diferentes Entes del Ministerio de Defensa y otra la estructura interna en la cual se brindan los servicios de red.

2.2.3.1 Topología Física

Desde el Centro de Conmutación quien es el encargado de brindar tanto el servicio de Internet como de Datos hacia los diferentes Entes del Ministerio de Defensa Nacional se cuenta con dos tipos de enlaces uno destinado para brindar el servicio a la red de internet y otro para brindar el servicio hacia la red de datos, distinguiéndose dos canales diferentes. Su topología se puede apreciar en la figura 31.

A nivel de red interna desde donde se proveen servicios de conectividad para los usuarios de la institución y acceso a los servidores de aplicaciones, su topología física se muestra en la figura 32.

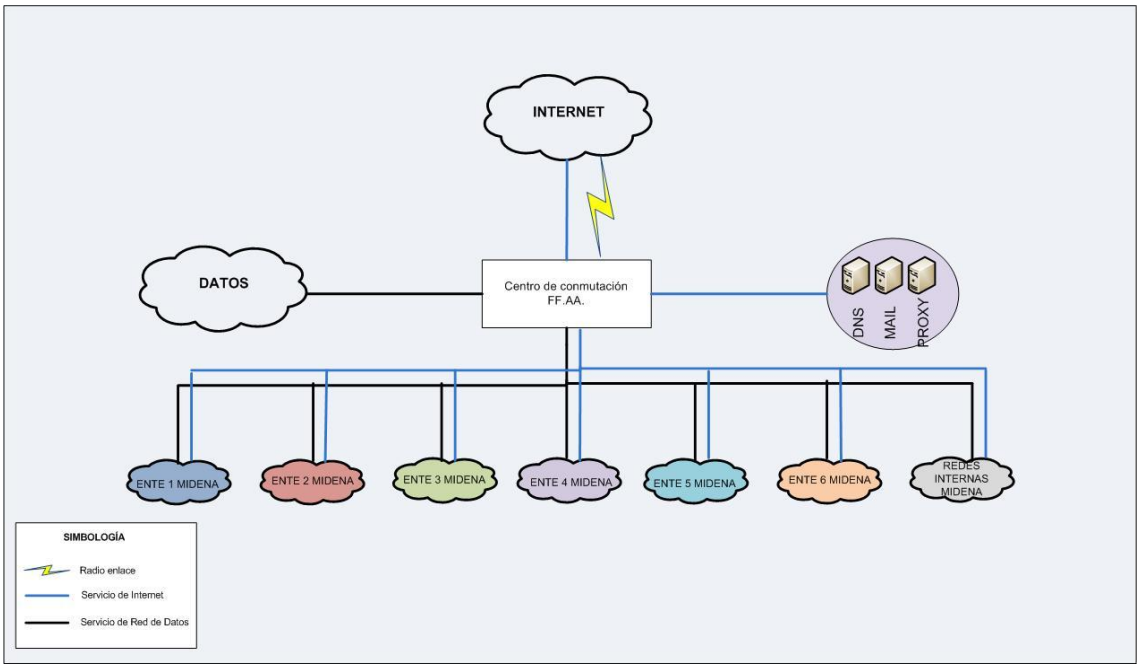


Figura 31. Topología Física Centro de Conmutación

Fuente: Nancy Yolanda Ramón I.

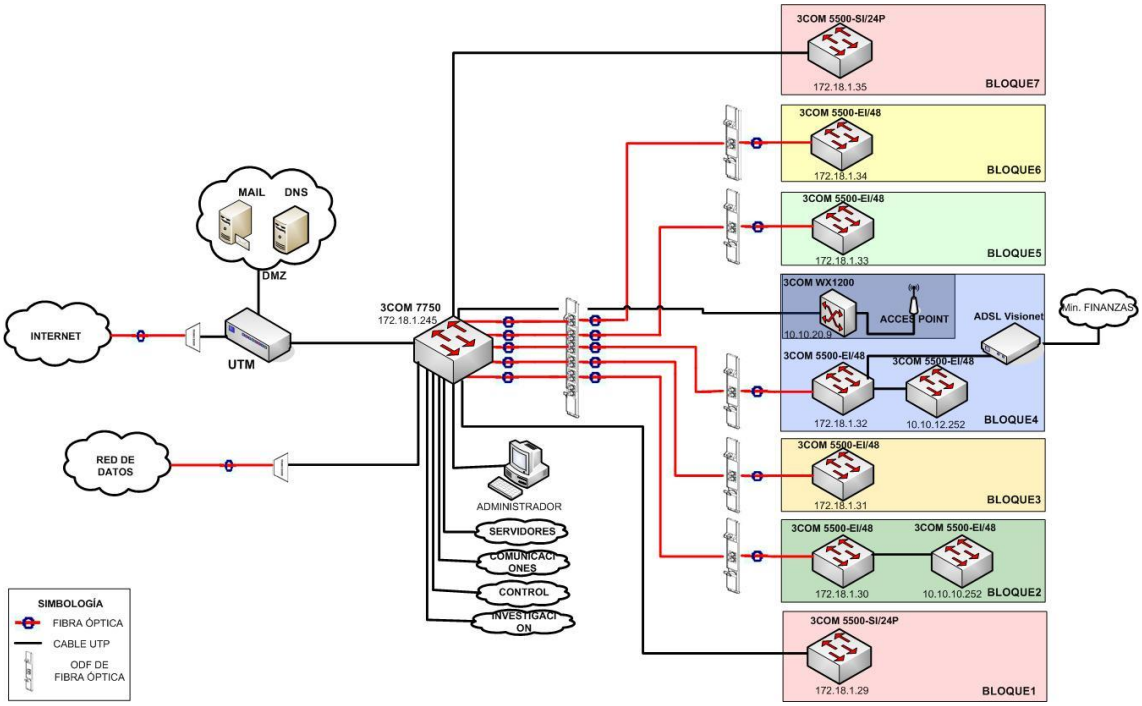


Figura 32. Topología física de la red interna

Fuente: Nancy Yolanda Ramón I.

2.2.3.2 Topología Lógica

La topología lógica de la red se encuentra establecida en base a un direccionamiento IP para cada una de las Vlans creadas en la institución. Su estructura lógica se puede observar en la siguiente figura:

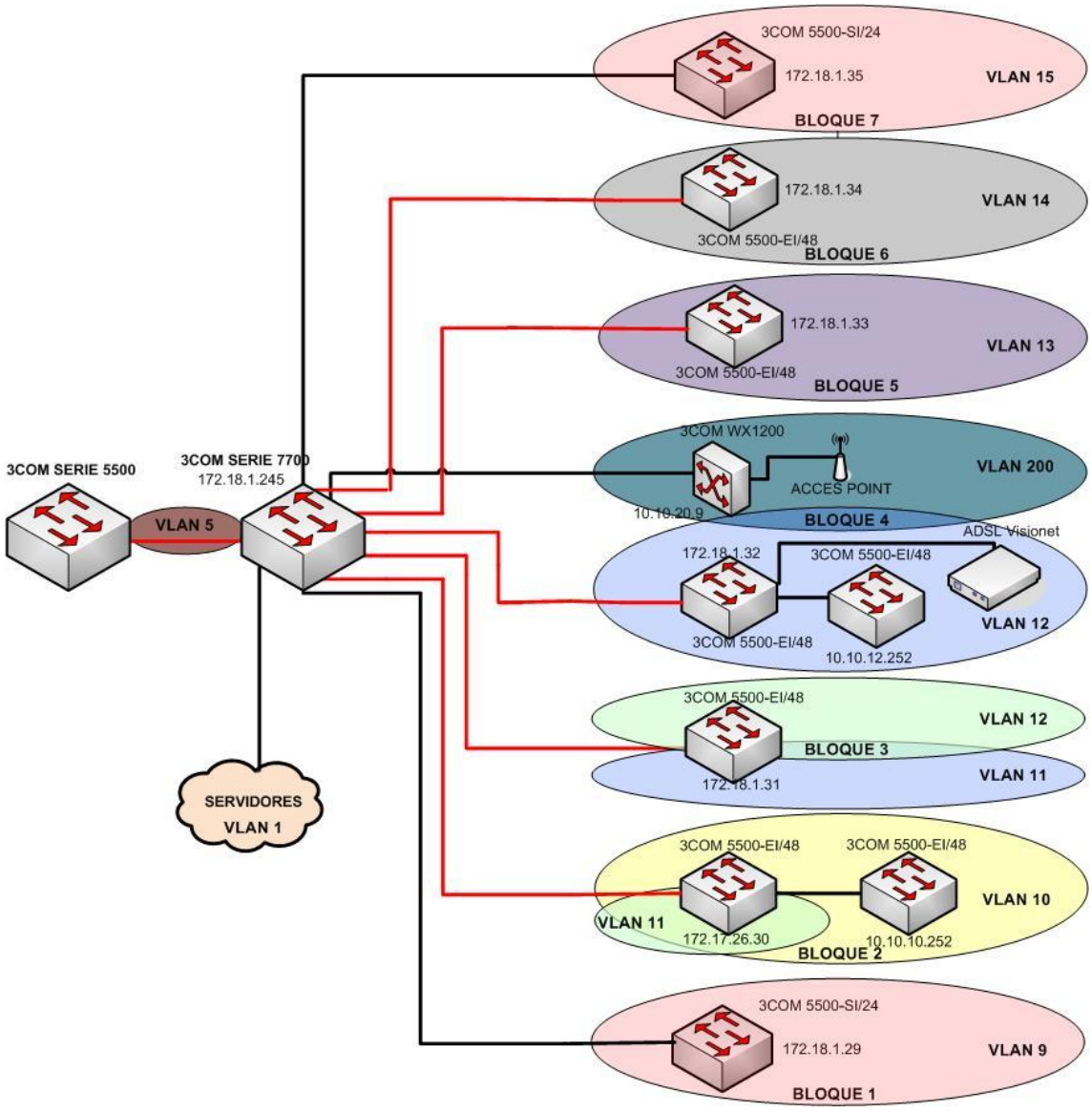


Figura 33. Topología lógica de la institución.

Fuente: Nancy Yolanda Ramón I.

2.2.4 ESPECTRO WIFI[83]

El análisis del espectro electromagnético realizado con AirMagnetSpectrum XT dentro del área de estudio muestra que se encuentran operando los canales 1, 6 y 11 a las frecuencias 2412 MHz, 2437 MHz, 2462 MHz respectivamente.

En la figura 34 se aprecian los canales en tiempo real con las respectivas potencias captadas en un promedio de -100 dBm.

[83] Wiki: Wireless Fidelity (Fidelidad inalámbrica)

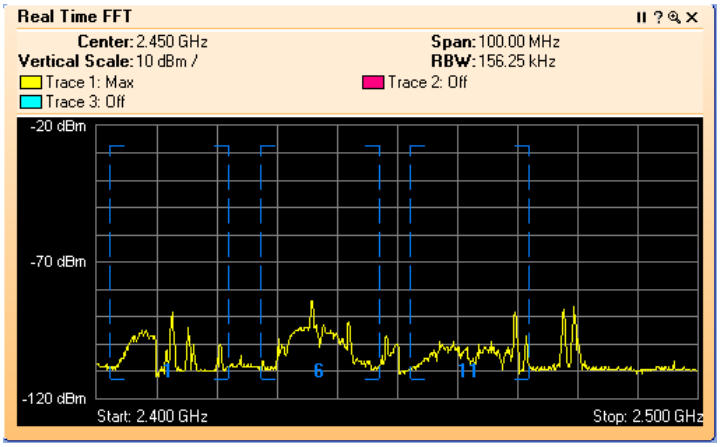


Figura 34. FFT en tiempo real

Fuente: Equipo de Prueba AirMagnetSpectrum XT

En la figura 35 se observa el barrido espectral y la utilización de las frecuencias en dBm. El color verde de la figura muestra la utilización de los canales, mientras que el color azul muestra la disponibilidad del espectro.

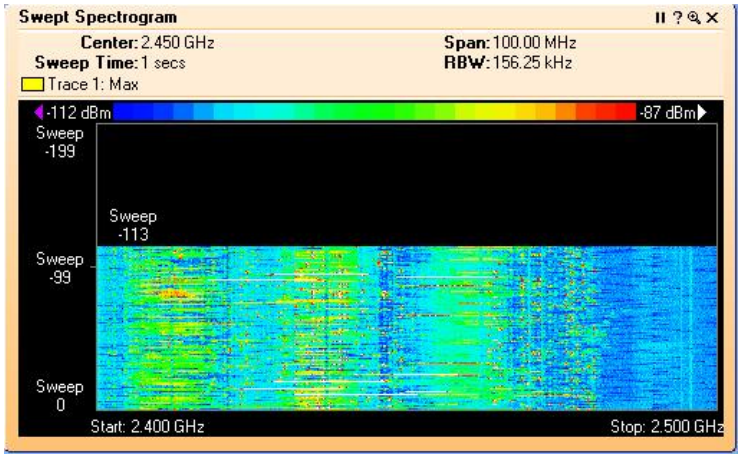


Figura 35. Barrido del espectro

Fuente: Equipo de Prueba AirMagnetSpectrum XT

2.3 ANÁLISIS DE SITUACIÓN ACTUAL

Con el levantamiento de información realizada es conveniente que se proceda a hacer el análisis de la misma, mediante la cual se permita detectar los puntos positivos y las falencias de la infraestructura actual de red.

2.3.1 CABLEADO ESTRUCTURADO

La infraestructura de red del edificio del Ministerio de Defensa cuenta con 400 puntos de red activos, los cuales brindan conectividad a los usuarios hacia la red interna y red externa de la institución.
Como parte del levantamiento realizado se actualizó la información referente a usuarios, funciones y perfiles asignados tanto para navegación como para Directorio Activo, complementado de esta manera la distribución de puntos de red; su detalle se muestra en el Anexo 1 "*Distribucion de Puntos de Red*".

2.3.1.1 Cableado Horizontal

- Las bandejas metálicas que se encuentran instaladas en los cuartos de telecomunicaciones no solamente soportan los cables de datos, sino, que además conducen los cables de energía eléctrica, lo cual puede causar problemas de interferencia electromagnética en los cables de datos. Además ni los cables de datos, ni los cables de energía eléctrica se encuentran debidamente organizados.
- Las canalizaciones realizadas con tubo conduit para la distribución del cableado horizontal hacia las salidas de usuario se encuentran saturadas; por lo cual estas canalizaciones no soportan adición de nuevos puntos de red.
- Las nuevas conexiones de cableado UTP realizadas, se encuentran sobre techo falso sin ningún tipo de protección, ni canalización, por lo que es necesario reinstalar estos puntos de red con las debidas canalizaciones y utilizando las bandejas de datos correspondientes de manera que se cumpla con las normas y estándares de cableado estructurado.
- Los cables que van desde el rack hasta las bandejas de techo horizontal no se encuentran instalados con las debidas canalizaciones y accesorios, lo cual puede causar tensiones excesivas sobre el cableado instalado; además se podría sobrepasar los niveles de curvatura permitidos para los mismos, afectando también a la estética de dichos cuartos.
- En el interior de los modulares ni los cables de datos ni los cables de energía eléctrica se encuentran tendidos respetando los canales

designados, al encontrarse mezclados pueden ocasionar problemas en el rendimiento de la red debido a la emisión de campo electromagnético por parte de los cables eléctricos en el cableado de datos. De ser factible es necesario que se valide e instale correctamente el cableado, caso contrario es necesario la utilización de tubería corrugada que evite estas emisiones.

- En algunos departamentos del edificio existen canaletas y cables instalados de forma no apropiada en techos falsos, pisos y paredes, esto a más de afectar a la estética del cableado de datos también expone a las conexiones al polvo y roeduras. Es importante tener en cuenta que la instalación de canaletas evita tropiezos o jalones imprevistos en los cables instalados.
- Existen puntos de red que tienen daños físicos como jacks sueltos, sin face plate, cajetines sueltos y cajetines rotos causantes de la disminución de puntos de red, problemas de conexión y/o reducción del performance de la misma.
- Existen puntos de red sin una debida etiquetación, lo cual dificulta su ubicación dentro del edificio; así también se pudo detectar que la etiquetación utilizada no es la más adecuada debido a que ésta no permite tener una idea clara de su ubicación y servicio prestado a breve vista.
- Teniendo en cuenta que en un inicio el uso de los sistemas informáticos no estaba masificado, con el crecimiento de usuarios dentro de la red se ha debido realizar nuevas conexiones hacia los switches de bloque. Algunas de estas conexiones se conectan directamente hacia el switch del cuarto de telecomunicaciones sin que éstos lleguen a patch panel y sin usar ductos, ni canaletas en su instalación. Estos factores coadyuvan a la disminución del performance en la red, además de esta manera se dificulta la identificación de las conexiones en el cuarto de telecomunicaciones al no contar con un punto de control en la red, así también el orden en los mismos se ve afectado.
- En la parte posterior del rack del Bloque 4, debido a un mal dimensionamiento de medidas en los cables de red, se encuentran colocados jacks flotantes y patch cords para reflejarse en patch panel

causando disminución de rendimiento en los cables de conexión; además este tipo de conexiones aumenta un punto de falla en el enlace.

2.3.1.1.1 Certificación de puntos de red

Para la determinación del estado de los puntos de red del edificio, se hizo meritorio la realización de pruebas de certificación de red con equipos destinados para ello. Para las pruebas desarrolladas se utilizó los certificadores de red Fluke Network, con los resultados obtenidos se realizó un análisis de la información recopilada con la ayuda del software de gestión LinkWare. Ver Anexo 3 "*Pruebas de Certificacion*".

2.3.1.1.2 Análisis de resultados

Luego de realizada la certificación de los puntos de red del edificio se procedió al análisis de los resultados obtenidos, para lo cual se determinó los puntos de red que pasaron o no las pruebas de certificación, representando los resultados obtenidos de forma estadística por cada uno de los bloques analizados.

BLOQUE 1

Cantidad de Puntos de red certificados:	**42**
Puntos de red que pasaron la certificación:	40
Puntos de red que no pasaron la certificación:	2

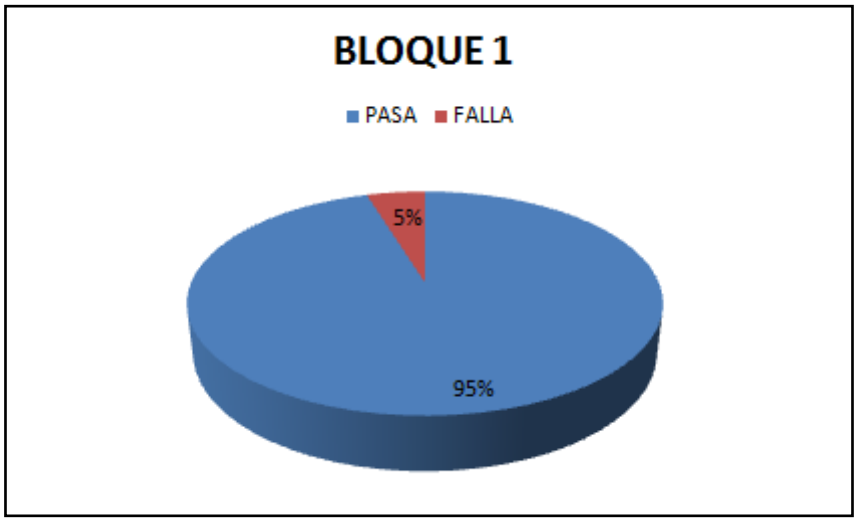


Figura 36. Certificación de puntos de red del Bloque 1

Fuente: Nancy Yolanda Ramón I.

BLOQUE 2

Cantidad de Puntos de red certificados:	**72**
Puntos de red que pasaron la certificación:	69
Puntos de red que no pasaron la certificación:	3

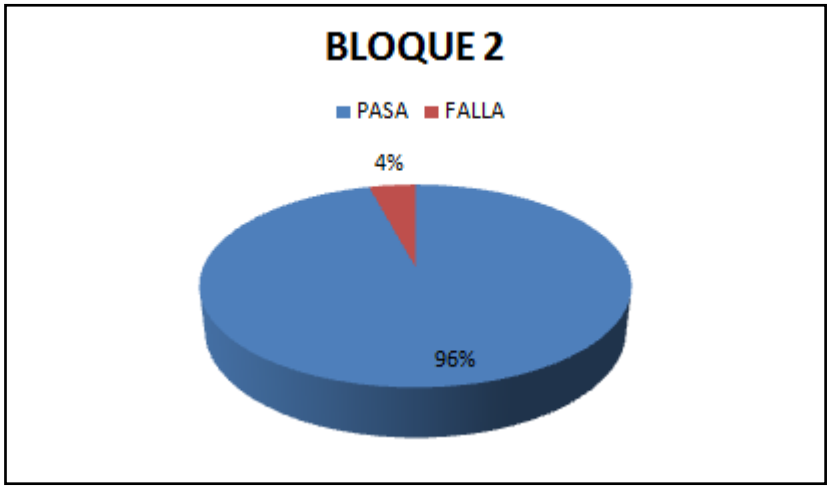


Figura 37. Certificación de puntos de red del Bloque 2

Fuente: Nancy Yolanda Ramón I.

BLOQUE 3

Cantidad de Puntos de red certificados:	54
Puntos de red que pasaron la certificación:	49
Puntos de red que no pasaron la certificación:	5

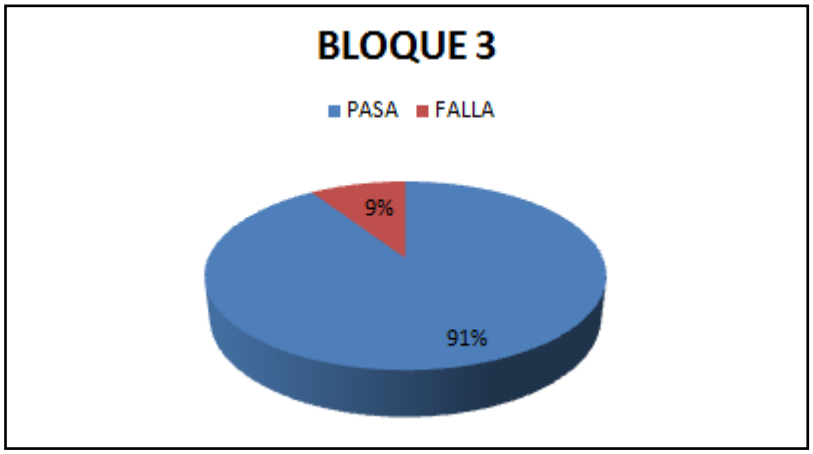


Figura 38. Certificación de puntos de red del Bloque 3

Fuente: Nancy Yolanda Ramón I.

BLOQUE 4

Cantidad de Puntos de red certificados:	**79**
Puntos de red que pasaron la certificación:	72
Puntos de red que no pasaron la certificación:	7

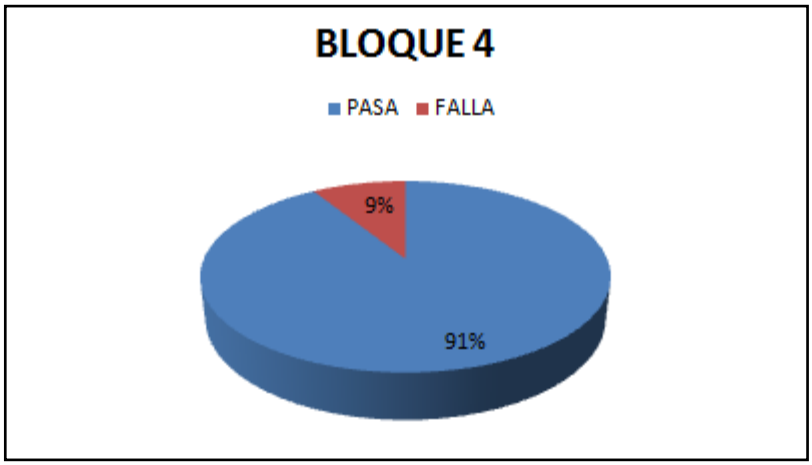


Figura 39. Certificación de puntos de red del Bloque 4

Fuente: Nancy Yolanda Ramón I.

BLOQUE 5

Cantidad de Puntos de red certificados:	**53**
Puntos de red que pasaron la certificación:	47
Puntos de red que no pasaron la certificación:	6

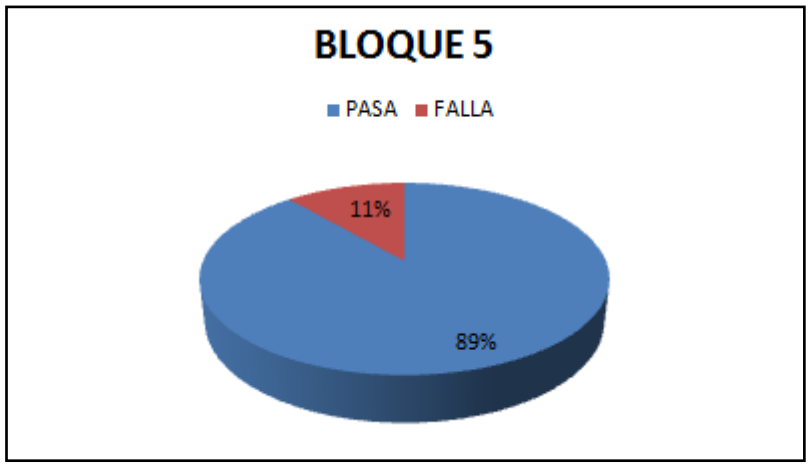


Figura 40. Certificación de puntos de red del Bloque 5

Fuente: Nancy Yolanda Ramón I.

BLOQUE 6

Cantidad de Puntos de red certificados:	**56**
Puntos de red que pasaron la certificación:	49
Puntos de red que no pasaron la certificación:	7

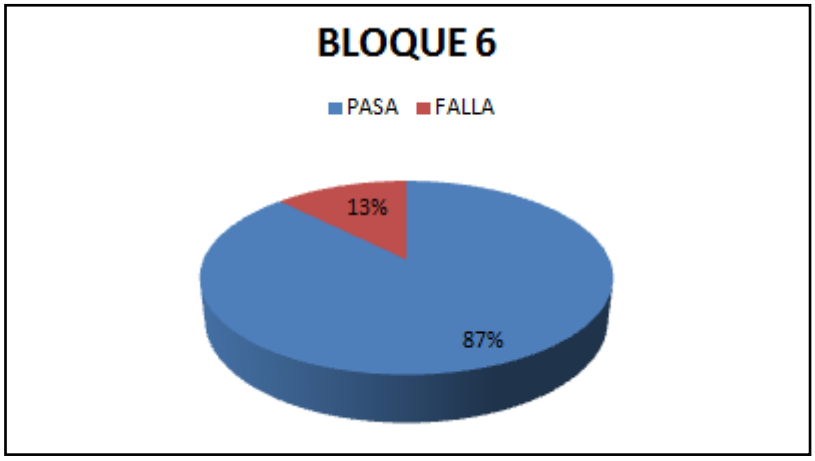


Figura 41. Certificación de puntos de red del Bloque 6

Fuente: Nancy Yolanda Ramón I.

BLOQUE 7

Cantidad de Puntos de red certificados:	**17**
Puntos de red que pasaron la certificación:	16
Puntos de red que no pasaron la certificación:	1

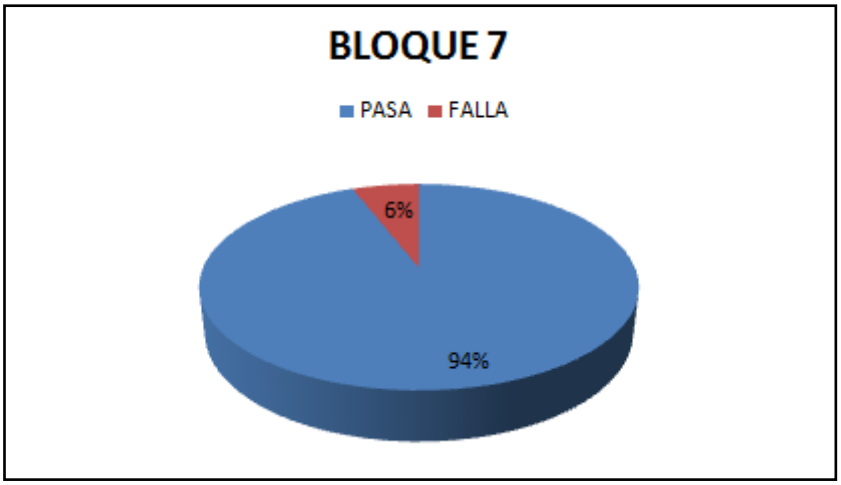


Figura 42. Certificación de puntos de red del Bloque 7

Fuente: Nancy Yolanda Ramón I.

REPORTE GENERAL DE CERTIFICACIÓN

Total de puntos certificados:	**373**
Total de puntos que pasaron la certificación:	342
Total de puntos que no pasaron la certificación:	31

En las siguientes figuras se observa el resultado del reporte total de forma estadística.

Figura 43. Resultado General de Certificación 1

Fuente: Nancy Yolanda Ramón I.

Las pruebas de certificación de red se realizaron a 373 puntos de red del edificio, de los cuales la mayor parte pasaron las pruebas de certificación, constituyendo esto un 92% de los puntos de red evaluados, y un pequeño porcentaje equivalente al 8% de puntos de red evaluados no pasaron la certificación debido a diferentes parámetros, los cuales se pueden apreciar en la siguiente figura:

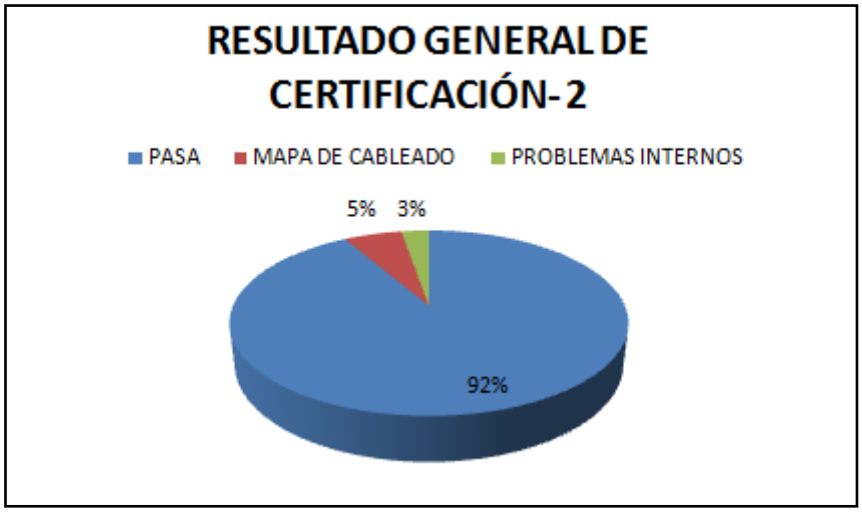


Figura 44. Resultado General de Certificación 2

Fuente: Nancy Yolanda Ramón I.

En la figura 44 se observa que del 8% de puntos de red que no cumplieron los parámetros de certificación, 5% de ellos corresponden a problemas con el mapa de cableado y tan solo un 3% de ellos tienen problemas internos referidos al NEXT, ACR y RL.

Posibles causas de los problemas para la certificación de los cables de red.

- El **mapa de cableado** puede fallar por: cortes a lo largo del cable, cables mal ponchados, jacks sin face plate o cables de red sueltos (al estar los jack sueltos estos pueden sufrir daños debido a una mala manipulación, o pueden ser pisados o incluso rotos). El uso inapropiado de canaletas y conectores finales o simplemente el obviar la instalación de algunos de ellos son causantes de problemas con el mapa de cableado.
- Las **pérdidas de retorno** pueden ser causadas por maltrato del cable durante su instalación, torceduras de los cables de red, curvaturas menores o iguales a 90 grados o el uso inapropiado de accesorios de cableado estructurado, además un factor influyente en el mismo es la longitud del enlace.
- La **interferencia por extremo cercano** puede darse por el destrenzado del cable, cortes en el aislante de los pares, ruptura de los hilos del cable, altas frecuencias de trabajo, así como también influye la longitud del enlace. Además este factor se ve alterado por fuentes de interferencia

electromagnética externas cercanas a los cables de datos (cajas eléctricas, motores, entre otros).

Del análisis de las pruebas de certificación, se deduce que la mayor parte del cableado estructurado del edificio se encuentra en buenas condiciones, por tanto el mismo puede seguir operando dado que al momento la red no demanda de mayores prestaciones, además teniendo en cuenta que los servicios que se ofrecen por la red son netamente de datos.

Considerando que de los puntos de red que no pasaron la certificación su mayor parte tienen problemas con el mapa de cableado por una o más de las causas indicadas anteriormente; estos problemas en su mayor parte puede ser resueltos reparando los mismos, de esta manera se habilita puntos de red y se aumenta a su vez la operatividad de la misma.

Cabe destacar que debido a que no se cuenta con una firma autorizada que acredite las pruebas de certificación realizadas, las mismas constituyen un documento que si bien cumple con todos los requerimientos técnicos, éstos necesitan ser avalados por una institución autorizada para que sea considerado como un informe válido.

2.3.1.2 Cableado Vertical

- El backbone vertical que conecta dos de los bloques del edificio es a través de cable UTP Categoría 5e, lo cual no ocurre con el backbone de los demás bloques en los cuales se utiliza fibra óptica como backbone vertical.
- El backbone instalado no cuenta con redundancia, por lo que si se produce un corte físico o cualquier otro daño a lo largo del backbone, se dejaría sin servicio a toda la red o parte de ella.
- La fibra óptica principal que llega a cada uno de los rack de telecomunicaciones de los bloques, no tiene ninguna protección, lo que la hace susceptible a daños físicos involuntarios o debido al mal manejo de la misma.

2.3.1.3 Área de trabajo

- En algunos de los departamentos las tomas de datos utilizadas como salidas en las áreas de trabajo no cuentan con la debida etiquetación, causando principalmente problemas para la administración del cableado estructurado del edificio.
- Ciertos face plates se encuentran sueltos o en mal estado, pudiendo ocasionar problemas en el mapa de cableado debido a la manipulación a la que se encuentran expuestos.
- Debido a la demanda de puntos de red algunas de las salidas destinas para el servicio de voz han sido utilizadas como salidas de datos, y viceversa, sin embargo en base al levantamiento realizado se puede mencionar que existe disponibilidad de puntos de red tanto de datos como de voz, por lo cual su uso no es el más adecuado, ya que de esta manera se afectan los servicios prestados y además se evidencia un desorden a nivel de los puntos de patch panel asignados.

2.3.1.4 Cuartos de Telecomunicaciones

- Cada uno de los bloques del edificio cuentan con un cuarto de telecomunicaciones lo cual facilita la administración y distribución del cableado de red.
- Los rack de cada uno de los bloques son tipo gabinete, los mismos que se mantienen cerrados bajo llave y su administración se encuentra a cargo del personal de Redes, permitiendo de esta forma llevar un control sobre el personal que ingrese a los mismos.
- Los racks poseen patch panel para voz y datos, sin embargo en algunos casos no se procede con el uso correcto. Ciertos puertos de voz se los está utilizando para datos y viceversa, afectando a la estética y administración de los mismos.
- En los racks no existen organizadores verticales y los organizadores horizontales existentes no son utilizados correctamente, por lo cual se evidencia desorden en los patch cord instalados.

- El mantenimiento de los cuartos de telecomunicaciones es deficiente, motivo por el cual existe gran cantidad de polvo, basura y residuos de cable en los mismos, lo cual afecta directamente al normal funcionamiento del equipamiento activo. Debido a que el edificio cuenta con ductos de ventilación, es necesario se realice un mantenimiento continuo para evitar que por medio de ellos circule polvo y basura residual.
- Las cajas eléctricas de dos de los cuartos de telecomunicaciones se encuentran mal instaladas ya que imposibilitan abrir totalmente la puerta del gabinete del rack. Además, en dichos cuartos existen cajas eléctricas abiertas que en algunos casos no son factibles cerrarlas ya sea debido a la gran cantidad de cables que salen de las mismas, o porque no cuentan con sus respectivas tapas.
- Dentro de los cuartos de telecomunicaciones pasan los ductos de la tubería de agua lo cual causa humedad a los mismos y puede provocar un acelerado deterioro del cableado.
- Las luminarias de los cuartos de telecomunicaciones son lámparas fluorescentes y se encuentran ubicadas a distancias no apropiadas de los racks. Las luminarias emiten campos electromagnéticos y al estar situados a cortas distancias de los racks, causan interferencia en la transmisión de los datos.
- En caso de fallas de energía no se cuenta con lámparas de emergencia dentro de los cuartos de telecomunicaciones, ni tampoco se tiene la señalética adecuada.
- Las bandejas horizontales y verticales soportan tanto el cableado de datos como el cableado eléctrico sin una debida organización de los mismos.

2.3.1.5 Data Center

- Los rack del Centro de Datos albergan los servidores de aplicación y el equipamiento activo en ambientes destinados para ello.
- Existe un sistema de aire acondicionado en el Data Center que permite que la temperatura se mantenga entre 20^0 y 23^0 C, constituyendo una temperatura óptima para su operación.

- Todo el equipamiento activo y servidores de aplicaciones se encuentran conectados a la red estandarizada, protegiéndolos ante fallos de energía.
- Todos los rack del edificio cuentan con una conexión hacia el sistema de puesta a tierra que los protege ante corrientes de fuga y sobrecargas eléctricas.
- Existe un UPS de 80 kVA que alimenta a los equipos de conmutación y servidores del Data Center en caso de fallas en la energía eléctrica. Adicionalmente se encuentran tres UPS que son utilizados para la red de comunicaciones.
- El mantenimiento del Data Center es deficiente por lo cual es recomendable realizar periódicamente su limpieza; además se debe utilizar de mejor manera la ductería, techo falso, piso falso y bandejas existentes para la distribución del cableado de datos y eléctrico. Así también se recomienda utilizar los accesorios apropiados para el manejo del cableado los cuales protejan de tensiones y ángulos inapropiados en el recorrido del mismo.

Existen cuatro racks en el Data Center que cumplen diferentes funciones:

- El primero es un rack tipo gabinete, en éste se encuentran los equipos de redes y telecomunicaciones como también 4 bandejas de fibra óptica (ODFs), un switch 3Com serie 7700, un UTM[84] marca Fortinet, un patch panel para la red de datos, un organizador horizontal de fibra óptica y dos organizadores horizontales para cable UTP; estos equipos permiten el funcionamiento de la red del edificio, al constituirse como el núcleo de la red interna.
- El segundo rack es de piso, aquí se encuentran los servidores Blade y su terminal, destinados a realizar actividades de monitoreo, inventario IP, servidores de aplicaciones, servidores de bases de datos y correo electrónico.
- El tercer rack es tipo gabinete, en este se encuentran los servidores de desarrollo, aplicaciones y DNS[85].

[84] UTM: Unified Threat Management (Gestión Unificada de Amenazas)
[85] DNS: Domain Name System (Sistema de Nombres de Dominio)

  - El cuarto rack es de piso, en el mismo se encuentran los servidores del Controlador de Dominio Primario y Secundario, además se encuentran los servidores de Base de Datos (Oracle), servidor de Aplicaciones y una consola de administración para todos los servidores.
- En el Data Center no se cuenta con las debidas señalizaciones y lámparas de emergencia en caso de fallos de energía, constituyéndose en un problema operacional y de administración.
- A pesar de que el Data Center cuenta con sensores de humo para protección ante la presencia de fuego, este no es el único problema al cual se encuentra expuesto este lugar; es recomendable que se instale un sistema de monitoreo digital el cual pueda alertar al personal ante la presencia de valores anormales en la temperatura, humedad relativa, condensación del aire, entre otros, de manera automática. Así también es recomendable implementar un sistema de monitoreo en tiempo real que permita tener el control y registro de las labores realizadas en el interior del mismo.

2.3.1.6 Sistema de puesta a tierra

- El sistema de puesta a tierra del edifico protege tanto a los servidores como al equipamiento activo del mismo.
- Se tiene una instalación de puesta a tierra tipo malla para protección de los equipos del Data Center, ante corrientes de fuga y sobrecargas eléctricas.
- Cada uno de los rack del edificio cuentan con una conexión al sistema de puesta a tierra, sin embargo esta conexión no se encuentra debidamente etiquetada.

2.3.2 ELEMENTOS DE PARTE ACTIVA

2.3.2.1 Equipos de red

- El equipo utilizado para brindar el servicio hacia las diferentes fuerzas es un equipo de capa 3 el cual realiza la función de enrutamiento de las diferentes redes a las cuales brinda el servicio. En el equipo utilizado se observa disponibilidad de puertos

- El equipo utilizado a nivel del núcleo de la red interna es un switch modulable y presenta disponibilidad de puertos; además de requerirse, este equipo cuenta con módulos disponibles para asignación de nuevas tarjetas de red, que permite ampliar la capacidad de puertos de red.
- Los switches utilizados a nivel de usuario final en la red interna soportan la carga del edificio, así también al ser equipos administrables permiten configurar los mismos adecuándose a las necesidades que demande la red. Sin embargo estos equipos cuentan con una configuración básica.
- El servicio de red inalámbrico es aplicado solo para el Bloque 4, debido a que únicamente se cuenta con un AP[86].
- La conexión mediante el modem ADSL utilizado por el Departamento de Compras Públicas implica un problema de seguridad para la red debido a que el mismo no está siendo controlado por un equipo de seguridad perimetral, así también ésta red debido a la configuración del equipamiento activo tiene acceso hacia toda la red interna, por lo cual es necesario tomar acciones al respecto, aplicando a nivel de red esquemas de microsegmentación.
- En los switches ubicados en los Bloques 3, 5 y 6 se observa gran densidad de puntos de red ocupados, existiendo poca disponibilidad ante el crecimiento futuro de la misma. Ver Anexo 2 "*Disponibilidad del Equipamiento Activo*".
- En los Bloques 2 y 4 del edificio se encuentran ubicados switches en cascada para dar servicio a ciertos departamentos o usuarios; debido a la demanda de puntos de red a nivel de usuario y escasez de puntos en el equipamiento activo principal se los ha utilizado para dar una solución rápida, sin embargo es necesario tener en cuenta que esto produce mayor tráfico a nivel de puertos e implica disminución en el ancho de banda, haciendo que la red se vuelva más lenta (dominios de broadcast). Además se debe tener en cuenta que en la mayoría de los casos es factible la ampliación de la red ya que a excepción de los bloques 3, 5 y 6 se tiene disponibilidad de puntos de red en los equipos de conmutación. Así

[86] AP: Access Point (Punto de Acceso)

también en lugar de realizar conexiones en cascadas es zrecomendable aplicar apilamiento a nivel del equipamiento activo.

- Existen equipos de conmutación y enrutamiento que no se encuentran en uso como se detalla en la tabla 10, los mismos que pueden ser utilizados en la red.
- El uso del CPU[87] de los equipos de conmutación es relativamente bajo como se indica a continuación:

Tabla 12. Uso de CPU de los switches

EQUIPO	USO DE CPU
Switch de Core	19%
Switch Bloque 1	16%
Switch Bloque 2	10%
Switch Bloque 3	12%
Switch Bloque 4	15%
Switch Bloque 5	10%
Switch Bloque 6	15%
Switch Bloque 7	12%

Fuente: Nancy Yolanda Ramón I.

Del análisis de la tabla 12 se deduce que los equipos trabajan con un bajo consumo de sus recursos, por ende la red todavía puede ser explotada con mayor cantidad de tráfico; en caso de que se sobrepase el 80% el uso del CPU de los equipos, se debería pensar en soluciones de equipos más robustos o realizar backups y balaceo de carga con otros equipos.

2.3.2.2 Equipos de Control y Seguridad

- La administración de los equipos de control de acceso por medio de huella dactilar (Fingertec AC900), se la realiza desde el Cuarto de Control ubicado en un bloque diferente al de la ubicación de los equipos, por lo cual se ha utilizado un cable de red conectado directamente a un puerto del switch de bloque para su administración. Esta conexión física ha sido necesaria realizarla debido a que la vlan a la que pertenece el cuarto de control es diferente a la vlan del bloque en el que se encuentran físicamente los equipos de control y seguridad.

[87] CPU: Central Processing Unit (Unidad Central de Procesos)

2.3.3 ESQUEMA DE LA TOPOLOGÍA DE RED ACTUAL

Para el análisis de la topología de la red de la institución su estudio se divide en dos partes, una su topología externa desde la cual se provee el servicio tanto para internet como para datos hacia los diferentes entes del Ministerio de Defensa y otra la estructura interna a la cual se brinda los servicios de red.

2.3.3.1 Topología Física

El Centro de Conmutación es el encargado de brindar tanto el servicio de Internet como de Datos y el que a su vez distribuye el servicio hacia los diferentes entes del Ministerio de Defensa Nacional; cada uno de los servicios se los brinda por interfaces de red diferentes, como se puede apreciar en la figura.

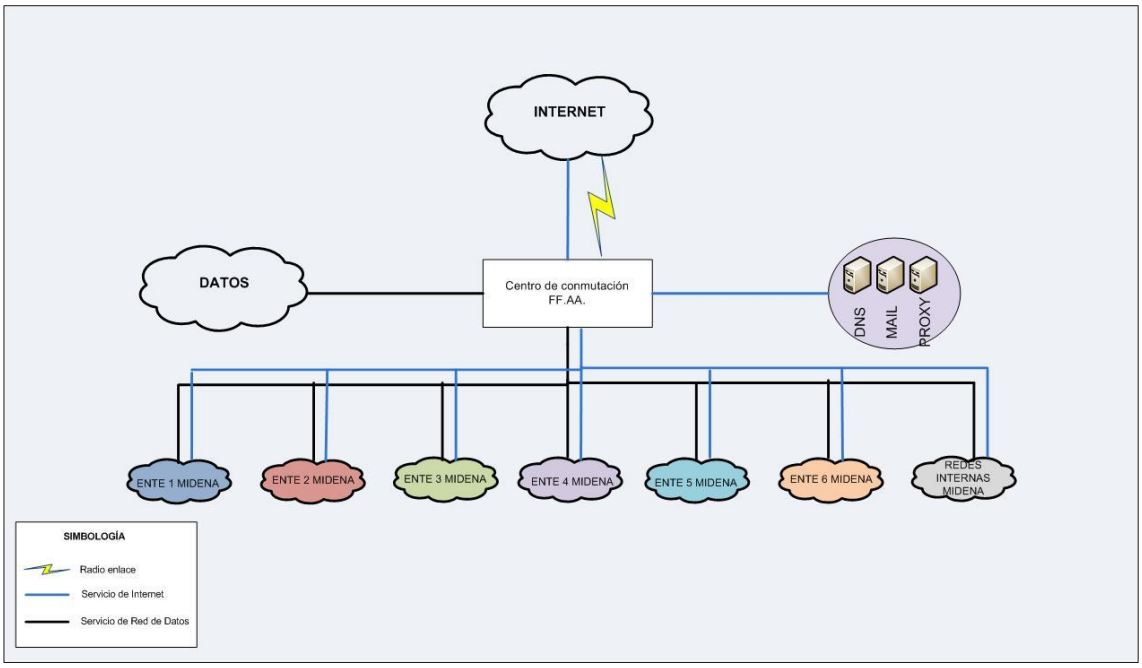


Figura 45. Topología física Centro de Conmutación

Fuente: Nancy Yolanda Ramón I.

La topología física de la red interna del Ente del Ministerio de Defensa en estudio cuenta con dos interfaces de entrada diferentes, una para el servicio de Internet y otra para la Red de Datos entregados por el Centro de Conmutación, los mismos que al pasar por el equipo de conmutación del edificio brindan el servicio a toda la red interna. En la siguiente figura se muestra la estructura física de la red de la Institución.

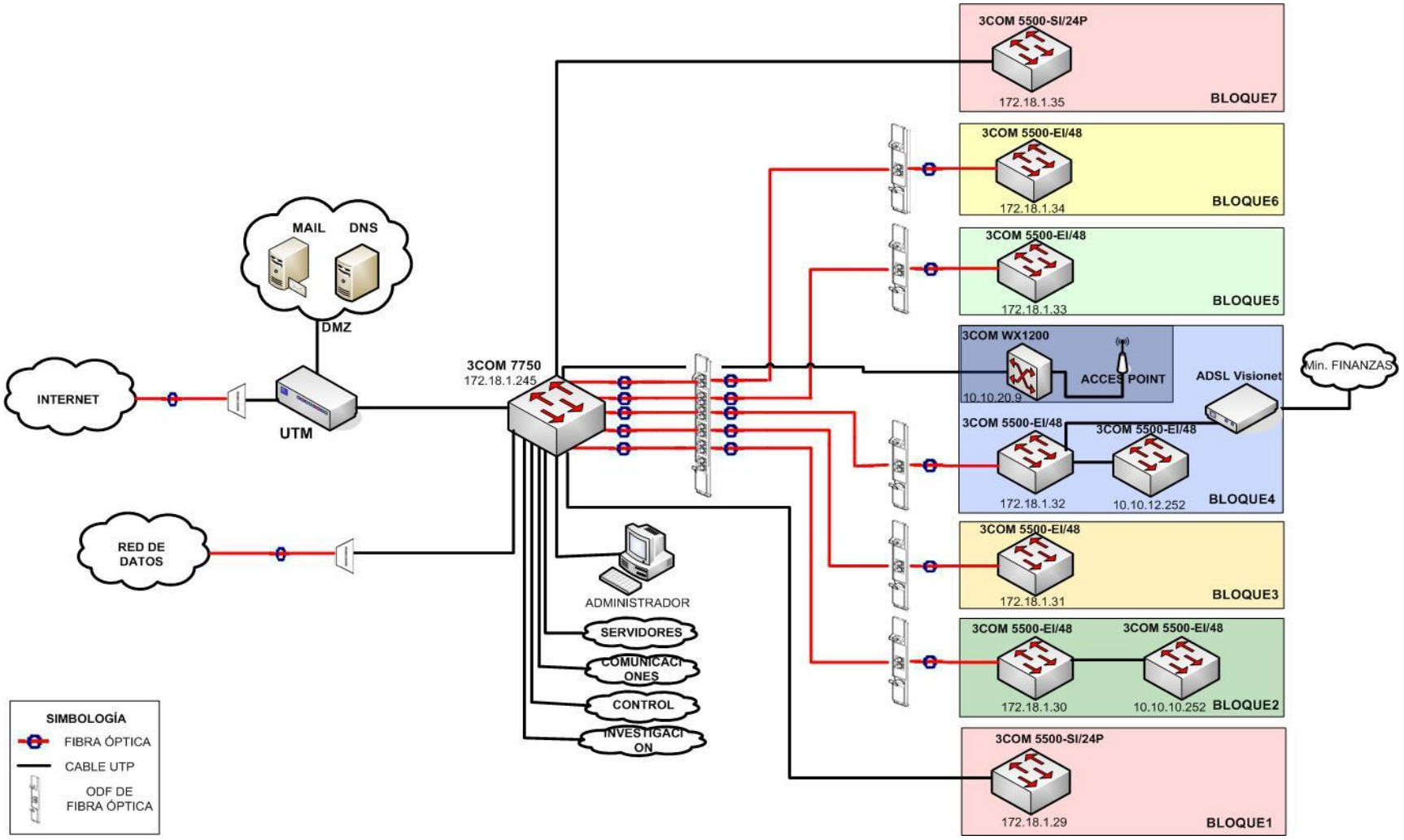


Figura 46. Topología física red interna

Fuente: Nancy Yolanda Ramón I.

Como se muestra en las figuras anteriores se pueden diferenciar tres redes: Red de Datos, Internet y LAN interna; las cuales están interconectadas por medio del switch 3Com serie 7700, como se detalla a continuación.

Red de Internet

- El proveedor actual del servicio de Internet del Ministerio de Defensa es TELCONET, el cual tiene dos medios físicos para brindar el servicio; uno de ellos brindado por medio del backbone de Fibra Óptica, y otro por medio de un radioenlace que se lo utiliza como backup. Estos medios físicos de internet los administra directamente el Centro de Conmutación del Ministerio de Defensa quién a su vez realiza la distribución del servicio hacia los diferentes entes del mismo.
- El servicio de Internet se distribuye para todos los entes del Ministerio de Defensa, utilizando como medio de transmisión Fibra Óptica. El enlace de fibra óptica hacia la institución llega a un equipo firewall UTM para luego pasar hacia el switch 3com serie 7700 del edificio ubicado en el Data Center y desde allí se distribuye el servicio para los diferentes departamentos del mismo.
- Hacia las redes de Comunicaciones e Investigación de la Institución se manejan enlaces directos; para su interconexión se reflejan en un ODF del Data Center para luego conectarse directamente hacia su respectiva red.

Red de Datos

- El backbone de la Red de Datos se encuentra ubicado en el Centro de Conmutación, ésta red se distribuye a los diferentes entes del Ministerio de Defensa por medio de enlaces de fibra óptica llegando al switch 3Com de la serie 7700 del Data Center del edificio, desde el cual se brinda el servicio de Red de Datos para los diferentes departamentos del mismo.

Red LAN interna

- En el Data Center del edificio se encuentra instalado el switch 3Com de la serie 7700 del cual se deriva el backbone vertical del edificio, conformado por 5 enlaces de fibra óptica que llegan hasta los ODFs ubicados en:

Bloque 2, Bloque 3, Bloque 4, Bloque 5 y Bloque 6 respectivamente. En el ODF de cada bloque están instalados patchs cords de fibra óptica que se conectan a los switches de acceso 3Com serie 5500. Además se tienen tres enlaces a través de cable UTP Cat 5e como backbone vertical utilizados para el Bloque 1, switch wireless ubicado en el Bloque 3 y para el Bloque 7. Así también en el switch 3com serie 7700 se hallan conectados los servidores de aplicaciones a través de patch cord de cable UTP categoría 5e.

- Dentro de la infraestructura de red del edificio se tiene switches en cascada tanto en la infraestructura del Bloque 2 como Bloque 4 conectados con patch cord de cable UTP categoría 5e.
- Desde el swich 3Com serie 7700 se tiene instalado un punto de red que va hacia el patch panel del Bloque 4, en el cual se encuentra conectado la PC del administrador de red. Este punto se lo utiliza con motivos de administración.
- Así también el edificio cuenta con una línea dedicada para uso del departamento de Compras Públicas, enlace brindado por medio de una conexión ADSL que se conecta directamente al switch 3Com serie 5500 de Bloque. El uso de ésta conexión no se encuentra limitada hacia el mencionado departamento pudiendo ocasionar problemas de seguridad por medio de este canal, como ataques a la red, denegación de servicio, intercepción, robo de la información o virus. En este Bloque también está instalado un switch wireless 3Com WX1200 conectado directamente al switch 3Com serie 7700, a éste se conecta un Access Point para dar servicio Wireless al departamento de Sistemas Tecnológicos.

2.3.3.2 Topología Lógica

- Con respecto a la topología lógica del edificio se ha establecido vlans a nivel de bloque como se muestra en la siguiente figura. Cada color representa a la vlan asignada en cada uno de los bloques.

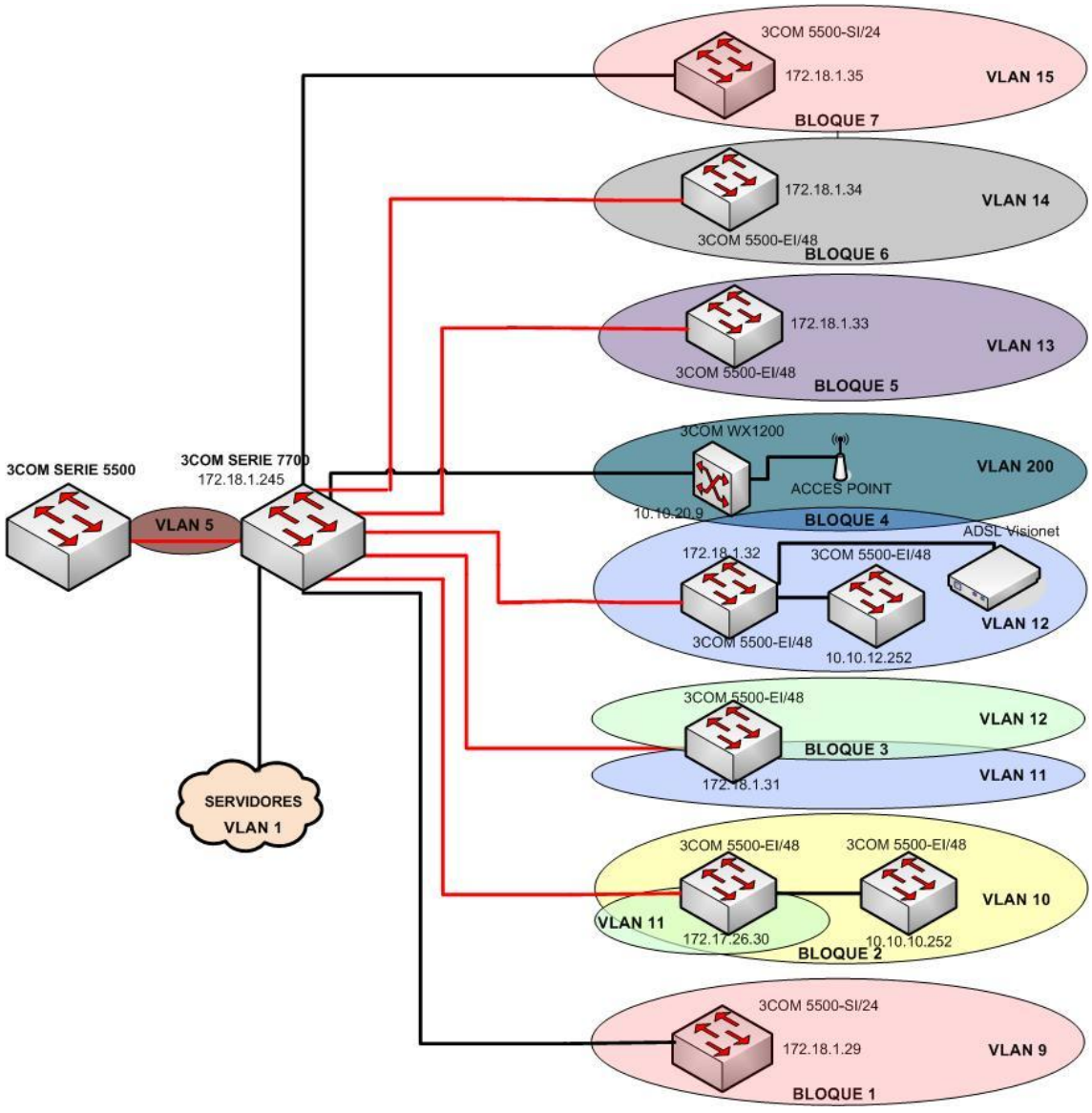


Figura 47. Topología Lógica de la red LAN

Fuente: Nancy Yolanda Ramón I.

- La configuración definida en los equipos de conmutación es la creación de vlans por cada uno de los bloques. En los Bloques 2 y 3 se comparten dos vlans debido a los requerimientos de los usuarios. Sin embargo se debe tener en cuenta que no se tiene un control inter-vlans ni tampoco su segmentación IP es la adecuada.
- Para el direccionamiento IP se utiliza subnetting, por lo cual no se tiene un direccionamiento eficiente provocando un desperdicio de las direcciones IP, a esto se suma la segmentación no adecuada y la falta de implementación de políticas en el tráfico interno.

- Dentro de las configuraciones de los equipos de conmutación se puede destacar lo siguiente:
    - Los equipos de conmutación se encuentran configurados con contraseñas de consola no seguras, además el acceso remoto se lo realiza vía Telnet, utilizando una conexión del tipo no segura.
    - Los equipos de conmutación tienen configurado tres tipos de usuarios: monitor, manager y admin; las contraseñas de manager y monitor son las contraseñas establecidas por defecto por el fabricante.
    - No se maneja políticas de control de seguridad a nivel de puertos, ni tampoco se controla el uso de las direcciones IP a nivel de usuario.
    - El switch 3COM serie 7700 ubicado en el Data Center del edificio, tiene la versión de software v3.01.50 de Agosto de 2005, en él se encuentran configuradas las siguientes VLAN:

Tabla 13. Lista de Vlan configuradas en el switch 3Com 7750

ID VLAN	NOMBRE
Vlan 1	SERVIDORES
Vlan 2	VOZ
Vlan 3	VIDEO
Vlan 9	BLOQUE 1
Vlan 10	BLOQUE 2
Vlan 11	BLOQUE 3
Vlan 12	BLOQUE 4
Vlan 13	BLOQUE 5
Vlan 14	BLOQUE 6
Vlan 15	BLOQUE 7
Vlan 110	NA
Vlan 111	NA
Vlan 112	NA
Vlan 200	WIRELESS
Vlan 300	EJERCITO
Vlan 301	EVALUACION

Fuente: Nancy Yolanda Ramón I.

Las VLAN mostradas se han asignado de manera que dan servicio al Bloque respectivo; así mismo se han configurado ACLs[88] básicas para permitir el tráfico desde algunas redes y restringir otras, sin

[88] ACLs: Access Control List (Listas de control de acceso)

embargo éstas no se encuentran asignadas, por lo cual al momento no brindan ningún servicio.

- Los cuartos de telecomunicaciones cuentan con switches 3Com de la serie 5500 con la versión de software v3.02.03s56 de Marzo de 2007 y la versión de software v3.02.00s56 de Junio de 2006. En ellos se tienen configuradas las siguientes VLAN.

Tabla 14. Vlan configuradas en los switches

Switches	Vlan ID	Nombre
BLOQUE 1	Vlan 1	SERVIDORES
	Vlan 9	BLOQUE 1
BLOQUE 2	Vlan 1	SERVIDORES
	Vlan 10	BLOQUE 2
	Vlan 12	BLOQUE 4
BLOQUE 3	Vlan 1	SERVIDORES
	Vlan 11	BLOQUE 3
	Vlan 12	BLOQUE 4
BLOQUE 4	Vlan 1	SERVIDORES
	Vlan 12	BLOQUE 4
BLOQUE 5	Vlan 1	SERVIDORES
	Vlan 13	BLOQUE 5
BLOQUE 6	Vlan 1	SERVIDORES
	Vlan 14	BLOQUE 6
BLOQUE 7	Vlan 1	SERVIDORES
	Vlan 15	BLOQUE 7

Fuente: Nancy Yolanda Ramón I.

Como se puede notar la segmentación de tráfico se encuentra realizada en base a cada Bloque y no en base a un estudio por dependencias.

- En los Bloques 2 y 4 se encuentran 2 switches conectados en cascada, provocando un aumento en los dominios de broadcast y desestabilidad de la red; al aumentar switches en cascada se disminuye el performance de la red y con ello también causa la disminución de la calidad de los servicios.

2.3.4 ANÁLISIS ESPECTRAL WIFI

Para la observación del comportamiento del espectro radioeléctrico se realizaron pruebas de monitoreo utilizando un analizador de espectros de frecuencias Wi-Fi, donde se detectaron redes inalámbricas operando en los canales 1, 6 y 11 los mismos que trabajan a las siguientes frecuencias:

- Channel 1: 2412 MHz
- Channel 6: 2437 MHz
- Channel 11: 2462 MHz

De las pruebas realizadas se concluye que los canales se encuentran operando de manera óptica según las especificaciones de las nomas IEEE 802.11b e IEEE 802.11g respetando la separación de los canales evitando que se produzcan interferencias entre los canales asignados, además se ha considerado valores reales desde los -70dBm a -120dBm.

2.4 INCUMPLIMIENTO DE NORMAS Y ESTÁNDARES DE CABLEADO ESTRUCTURADO [13-16]

Basados en las normas y estándares de cableado estructurado, durante el levantamiento de información se detectó el incumplimiento de algunas de ellas. Las más importantes se enumeran a continuación:

2.4.1 CABLEADO HORIZONTAL

- La norma ANSI/EIA/TIA 568 B establece:
  - No deben existir empalmes a lo largo del cableado horizontal, sin embargo debido al mal dimensionamiento de los cables se ha colocado jacks flotantes y patch cords para reflejarse en el patch panel.
  - Todas las conexiones realizadas hacia el área de trabajo deben ser correctamente protegidas, además las mismas no deben causar inconvenientes o problemas para los usuarios, pero algunas de las conexiones nuevas no tienen las debidas canalizaciones ni ductos necesarios como se detalló anteriormente.

  - Se debe tener un máximo de llenura en los conduit instalados del 40%, sin embargo se permite hasta un máximo de llenura del 60% cuando se han debido realizar adiciones no planeadas luego de la instalación inicial, no obstante, los conduit instalados en el edificio no permiten adición en los mismos y algunos de los cables de red instados no cuentan con ningún tipo de protección, por lo cual para las nuevas conexiones que se realicen y las que se deban modificar, es necesario tener en cuenta la aplicación de la norma.
- La norma 606A indica el uso de etiquetas que aseguren su clara identificación y lectura de los puntos de red y de todas las conexiones realizadas, sin embargo durante el levantamiento de información se encontraron 30 puntos de red sin la debida etiquetación, así también algunos de los puntos de red que si bien cuentan con una etiqueta, éstas no son las más adecuadas debido a que su lectura puede ser confundida o en muchos casos ilegible, al no haberse utilizado los materiales adecuados.

2.4.2 CABLEADO VERTICAL

- Norma ANSI/EIA/TIA 569
  - Se debe usar conduit para proteger la fibra óptica o cable UTP utilizado como cableado de backbone, sin embargo el cableado vertical del edificio no cuenta con protección física alguna.
  - Es necesario contar con diversos puntos de entrada para proveer el servicio de telecomunicaciones, asegurando la no interrupción del servicio por falla en la ruta. Al momento no se cuenta con redundancia del backbone principal por lo cual de existir una falla del canal, la red quedaría parcial o totalmente fuera de servicio.

2.4.3 CUARTOS DE TELECOMUNICACIONES

- En los cuartos de telecomunicaciones las luminarias instaladas y los cables de energía eléctrica no cumplen la norma ANSI/EIA/TIA 569 en donde se especifica los requisitos mínimos para separación entre circuitos de alimentación (120/240V, 20 A) y cables de telecomunicaciones:

  - Los cables de telecomunicaciones deben estar separados físicamente de los conductores de energía eléctrica;
  - Si dichos conductores pasan por la misma canaleta o bandeja deben estar separados por barreras entre el cableado lógico y eléctrico;
  - Dentro de las cajas de distribución o compartimentos de tomas, debe haber separación física total entre los cableados.

    Del levantamiento realizado se ha detectado su incumplimiento ya que en muchas de las bandejas de distribución, el cableado tanto de datos como de energía eléctrica se encuentra por las mismas bandejas sin ninguna organización, ni separación física en los conductores.

- Para reducir el acoplamiento de ruido producido por cables eléctricos, fuentes de frecuencia de radio, motores y generadores de energía eléctrica, se deben considerar las siguientes precauciones:
  - Uso de protectores contra irrupción en las instalaciones eléctricas para limitar la propagación de descargas.
  - Uso de canaletas o conductos metálicos, totalmente cerrados y puestos a tierra, o uso de cableado instalado próximo a superficies metálicas puestas a tierra.
- Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.
- Se debe emplazar instalaciones secas de supresión de fuego para contrarrestar los peligros de incendios en los mismos.
- Como retardante del fuego se recomienda cubrir un mínimo de una de las paredes con plywood de 19mm, de preferencia sin vacíos, con 2.4m de alto y bien fijado a la pared.
- Se deben instalar luces y señales de emergencia, emplazadas de manera que no se obstaculice la salida de emergencia. La señalización usada en los cuartos de telecomunicaciones debe ser desarrollada en base a un plan de seguridad del edificio.

2.4.4 DATA CENTER

- Se debe contar con diversos puntos de entrada para el servicio de telecomunicaciones, asegurando la no interrupción del mismo por falla en la ruta del enlace, permitiendo la continuidad de servicio y las necesidades existentes. Adicionalmente se deben escoger vías alternas para su instalación.
- Dentro del Data Center se deben considerar medidas de supresión de fuego secas, previniendo de esta manera riesgo de incendios y daños en el equipamiento.
- Se debe tener en cuenta medidas contra la filtración de agua, además, de existir riesgo de inundación se recomienda instalar desagües de piso, adicionalmente es necesario la instalación de un sistema de monitoreo constante para detectar cualquier anomalía.
- El Data Center debe tener un control y mantenimiento adecuado. Los pisos, paredes y techo deben ser tratados con productos especiales para eliminar el polvo, así también el suelo debe tener propiedades antiestáticas.
- Se recomienda que un mínimo de una de las paredes del Data Center deben estar cubiertas con plywood de 19mm, de preferencia sin vacíos, a una altura de 2.4m y bien fijado a la pared, su uso actúa como un retardante ante la presencia de fuego.
- Las puertas deben ser de mínimo 0.9 metros de ancho y dos metros de altura, y con facilidad de remoción.
- Es necesario realizar un estudio de la carga permitida por el piso, de manera que la concentración de equipos no exceda el límite de carga por metro cuadrado.
- Se debe contar con una operación continua del sistema de aire acondicionado o sistema de enfriamiento. La temperatura y humedad debe ser controlada proveyendo una continua operación entre los rangos de 18ºC a 24ºC con 30% a 55% de humedad relativa. Estas medidas deben ser realizadas a 1,5 m del suelo.
- Se deber instalar luces y señales de emergencia, las cuales deben ser emplazadas sin obstaculizar la salida de emergencia. La señalización usada

en los cuartos de telecomunicaciones debe ser desarrollada en base a un plan de seguridad del edificio.

2.5 PARÁMETROS DE RENDIMIENTO DE LA RED ACTUAL

Dentro del levantamiento de información es importante tener en cuenta los parámetros para medir el rendimiento de la red actual como los que se detalla a continuación:

2.5.1 FLEXIBILIDAD

La red del edificio del Ministerio de Defensa maneja una estructura de topología en estrella, mediante la cual se facilita la adición, modificación o eliminación de puntos de red. Aunque su topología de red soporta nuevos cambios el equipamiento en muchos casos no lo soporta.

2.5.2 DISPONIBILIDAD

Aunque actualmente en la red no existen mecanismos para determinar la disponibilidad de la misma, esta no puede brindar una disponibilidad total a nivel de red debido a que:

- La conexión tanto hacia la red de datos como de internet depende de enlaces externos hacia el Centro de Conmutación del Ministerio de Defensa, los cuales al no contar con canales redundantes pueden producir caídas del servicio al presentarse algún fallo en el enlace, el mismo que de ser considerable puede dejar sin servicio a toda la red interna por el tiempo en que este tarde en resolverse.
- A nivel de la red interna no se cuenta con enlaces redundantes hacia los principales equipos de conmutación por lo cual de producirse daños o problemas en su conexión la red quedaría parcial o totalmente fuera de servicio.
- El equipamiento de red de los niveles críticos como núcleo y distribución no cuentan con redundancia por lo cual de presentarse algún problema en alguno de ellos se interrumpiría el servicio de red de manera parcial o total.

Sin embargo es necesario considerar que en caso de fallas de los canales físicos o de los equipos de conmutación internos la red quedaría fuera de servicio, caso contrario es importante considerar lo siguiente:

- La capacidad de procesamiento de los servidores utilizados es la adecuada para el manejo de tráfico generado, por lo cual no se presenta interrupción en el servicio prestado hacia la red de datos.
- El backbone vertical se lo realiza a través de fibra óptica y cable par trenzado Cat 5e, los mismos que soportan el tráfico que fluye por la misma.
- En caso de fallas del suministro de energía local se cuenta con UPS que evitan los cortes de energía en la red, por tanto se asegura su operatividad.

2.5.3 ESCALABILIDAD

El equipamiento del edificio del Ministerio de Defensa Nacional como se puede observar en el Anexo 2 "*Disponibilidad de Equipamiento Activo*", presenta factibilidad de crecimiento de usuarios en la red a excepción de los Bloques 3, 5 y 6 que se encuentran con una capacidad limitada de crecimiento debido a que existen pocos puntos de red libres.

Es importante considerar que el equipamiento que se maneja posee características escalables ya que permite apilar hasta ocho switches de las mismas características, con lo cual se solucionaría el inconveniente de disponibilidad de puntos de red.

2.5.4 RENDIMIENTO

Todo el equipamiento de red del edificio es administrable, además su capacidad de procesamiento permite manejar grandes cantidades de tráfico como se determinó anteriormente, así también el uso de CPU se encuentra en niveles muy bajos lo cual indica que se puede manejar niveles más altos de tráfico sin ningún tipo de inconveniente.

Es importante considerar que el equipamiento que se maneja a nivel interno es de gama alta, el cual como se determinó soporta nuevas aplicaciones de red.

2.5.5 DOMINIOS DE BROADCAST

Los dominios de Broadcast del edificio se los encuentra definidos en base a bloques, más no en base a un estudio por dependencias o funciones, el cual no es óptimo. Es importante considerar que al no manejar políticas de control de tráfico no se limita el tráfico a la vlan respectiva.

2.5.6 SEGURIDAD

- Al no existir esquemas de microsegmentación de red y ACLs para restringir el tráfico intervlan no existe un control del tráfico que circula en la red; el mismo se encuentra abierto hacia todo el segmento de red manejado en el edificio.
- No existen políticas definidas a nivel de puertos del equipamiento activo para limitar el uso de los mismos a una solo dirección MAC e IP, por lo cual al momento, más de un equipo de cómputo puede utilizar un mismo punto de red sin que se tenga un control de esto. Las personas que conocen el procedimiento para cambiar la configuración de una tarjeta de red, podrían configurar a otro equipo o incluso al mismo con una dirección diferente a la asignada lo cual desemboca en un uso indiscriminado del direccionamiento IP; al no existir políticas bien definidas sobre el uso de la red, no se puede establecer sanciones cuando se incurra en el incumplimiento de normas del uso de la red.
- La seguridad de la red radica en tres mecanismos de Seguridad como son: el Firewall UTM, Directorio Activo y Servicio de antivirus.
    - El primer elemento el servidor UTM protege a la red ante accesos no autorizados, sin embargo existe el inconveniente que al ser un equipamiento licenciado si no se contrata el servicio de renovación de licencia puede quedar la red fuera de servicio.
    - El segundo elemento el Directorio Activo realiza un control de acceso de los usuarios hacia la red por medio del ingreso de usuario y contraseña para su acceso, sin embargo no todas las máquinas se encuentran autenticadas al dominio de la institución por lo cual no se tiene un control total de la misma. Así también no se tiene un control

adecuado de las políticas aplicadas, debido a que el personal no se encuentra debidamente capacitado para su administración.

  - El tercer elemento es el antivirus que protege a la red ante proliferaciones de virus, gusanos, troyanos, entre otros, este servicio muchas veces a causado graves inconvenientes debido a que no se ha dado soluciones rápidas ante proliferaciones de nuevas amenazas y al no contar con una segmentación adecuada de la red, estos se propagan sin ninguna limitación causando inconvenientes en la red.

- El acceso hacia los equipos de conmutación no se encuentra debidamente configurado ya que al contar con diferentes niveles de acceso como se explicó anteriormente y al permitirse el acceso por medio de sesiones no seguras, alguna persona con intenciones maliciosas podría ingresar a los mismos y realizar cambios o modificaciones de las configuraciones ocasionando la denegación del servicio, entre uno de sus inconvenientes.

CAPITULO III. DISEÑO DE TOPOLOGÍAS FÍSICA Y LÓGICA PARA LA RED DE DATOS

3.1 INTRODUCCIÓN

El desarrollo del presente capítulo muestra el diseño para la red de datos de la institución, el cual enumerará aspectos relevantes a tomarse en cuenta para su implementación. Antes de realizar el rediseño de la red de datos, es importante considerar aspectos fundamentales para el mismo como son la proyección del crecimiento de la red, las políticas de red manejadas en su interior y los requerimientos de los usuarios de la infraestructura.

3.2 ESTUDIO DE LA PROYECCIÓN DE CRECIMIENTO DE RED EN LA INSTITUCIÓN

Para el estudio de la proyección de crecimiento de red en el edificio del Ministerio de Defensa se ha tomado como base la información brindada por el Departamento de Sistemas, en función de la cual se determinó que su crecimiento no se basa en el aumento del personal, debido a que la institución no tiene incrementos del mismo con el paso de los años (para determinar la necesidad de contratación de nuevo personal es necesario modificar su estructura orgánica), ya que el número de plazas de trabajo es fijo. Sin embargo, la masificación del uso de las TIC ha demandado la instalación de más puntos de red, previendo alcanzar un número máximo igual al número del personal contratado.

Se estima que para el siguiente año se cuente con 550 puntos de red de datos, teniendo de esta manera una infraestructura completamente operativa; para esto es necesario considerar que un crecimiento en la infraestructura de cableado estructurado lleva consigo la demanda de equipamiento de red.

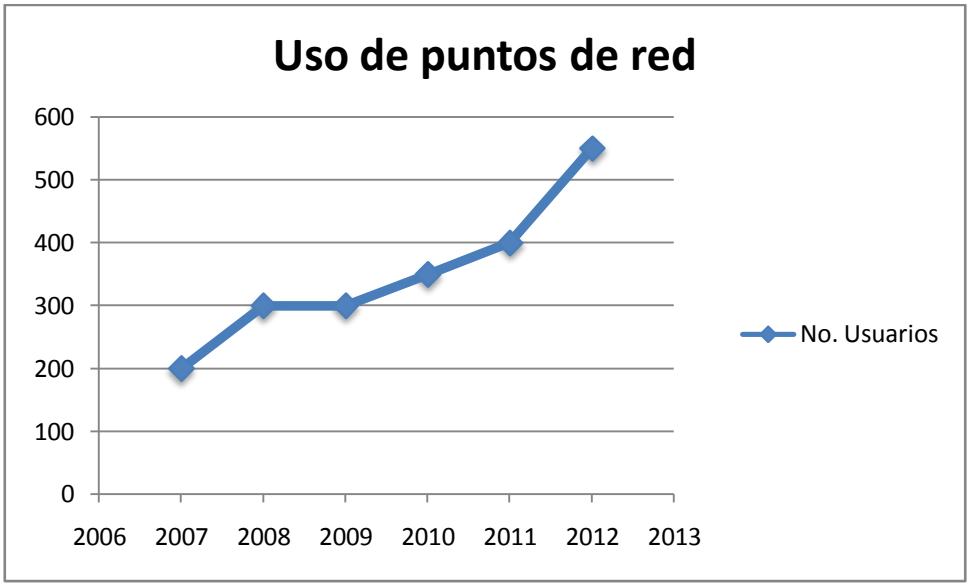


Figura 48. Estudio de proyección de crecimiento de usuarios de la red

Fuente: Nancy Yolanda Ramón I.

3.3 POLÍTICAS EN LA RED

Actualmente la red del edificio no cuenta con políticas definidas sobre el uso de la misma, sino más bien esta se rige en base a un conjunto de normas predefinidas por parte de la Dirección de Sistemas[89], quienes son los responsables de la infraestructura de red. Dentro de las normas de red implementadas se tiene:

3.3.1 CUARTOS DE TELECOMUNICACIONES

- El acceso hacia los cuartos de telecomunicaciones se encuentra restringido al personal de Administradores de Red, quienes son los encargados de manejar las llaves de las puertas de ingreso a los mismos. Si el personal de administración de la red telefónica necesita ingresar a los cuartos de telecomunicaciones, éstos deben solicitar su ingreso al personal de administración de red del edificio.

3.3.2 DATACENTER

- El acceso hacia el Data Center está limitado al personal de administración de la red; así también la administración de los diferentes sistemas de

[89] Fuente: Entrevista realizada al personal de administradores del Departamento de Sistemas.

aplicación de la Institución están restringidos al personal de Informática del área de Redes y Desarrollo.

- Sólo personal autorizado puede ingresar hacia el Data Center, quienes deberán portar las respectivas tarjetas de ingreso.
- Todo acceso hacia el Data Center debe ser registrado en el libro destinado para ello, indicando los nombres de las personas que ingresen, la hora tanto de entrada como de salida y el trabajo realizado en el mismo.

3.3.3 EQUIPAMIENTO ACTIVO Y SERVIDORES

- Las contraseñas de administración del equipamiento activo deben ser manejadas de forma exclusiva por los administradores de red de la institución.
- Las contraseñas de los servidores de aplicaciones deben ser manejadas de forma exclusiva por el personal de administración de los sistemas, con conocimiento del supervisor de la sección.

3.3.4 RED INALÁMBRICA

- La red inalámbrica del edificio es utilizada por el departamento de Sistemas con fines de capacitación, luego de lo cual la misma permanecerá deshabilitada.

3.2.5 EQUIPOS DE CÓMPUTO

- Todos los equipos de cómputo de la Institución deberán formar parte del directorio activo.
- Cada usuario contará con su respectiva cuenta de usuario y contraseña para el ingreso hacia los equipos computacionales.

3.4 ANÁLISIS DE REQUERIMIENTOS DE USUARIOS

Antes de realizar el diseño de la red de datos de la Institución es necesario determinar los requerimientos para la red por parte de los usuarios de la misma, de manera que el diseño realizado sea funcional. Dentro de los requerimientos de red reportados por los usuarios durante el levantamiento de información se tienen:

Adición de puntos de red: teniendo en cuenta la masificación de las TIC`s, es necesario estudiar los requerimientos de cada uno de los departamentos para determinar de esta manera la necesidad de adición o modificación de puntos de red.

Por varios de los motivos indicados en el capítulo anterior se precisa la implementación de nuevos puntos de red, su resumen en base a los bloques del edificio se muestra en la siguiente tabla:

Tabla 15. Resumen de requerimientos de red de la institución

BLOQUE	REQUERIMIENTO
Bloque 1	10 puntos de red
Bloque 2	11 puntos de red
Bloque 3	8 puntos de red
Bloque 4	20 puntos de red
Bloque 5	11 puntos de red
Bloque 6	18 puntos de red
Bloque 7	5 puntos de red

Fuente: Nancy Yolanda Ramón I.

Acceso a la red inalámbrica: es preciso considerar la necesidad de habilitar el servicio de red inalámbrica concebida con motivos de reuniones o capacitaciones en los diferentes salones dispuestos para ello.

Acceso a las aplicaciones: cada uno de los nuevos puntos de red que se instalen en el edificio deben tener acceso hacia todas las aplicaciones internas. El detalle de los servidores y aplicaciones contenidas se muestran a continuación:

- Servicio de antivirus
- Correo electrónico institucional
- Acceso a los portales web institucionales internos y de las fuerzas
- Acceso al portal web de intranet
- Sistema documental
- Sistema de inventarios

- Directorio Activo
- Acceso a Internet (en función de la necesidad, autorizada por el ente rector)
- Servicio de impresión
- Servicio de compartición de archivos
- Servicio de resolución de nombres interno

Así también el acceso hacia las aplicaciones de la red interna como externa deben ser fiables y confiables, mejorando su velocidad de acceso y asegurando su disponibilidad.

3.5 REINGENIERÍA DE LA RED DE DATOS DEL EDIFICIO DEL MINISTERIO DE DEFENSA

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

Así también el diseño propuesto mejorará 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 y a nivel de la parte activa como se aprecia más adelante.

3.5.1 CONSIDERACIONES DE DISEÑO

3.5.1.1 Cableado Estructurado

Es importante tener en cuenta aspectos relacionados al cableado estructurado ya que el funcionamiento lógico de la red depende de su parte física. A continuación se recogen algunas de las consideraciones para el diseño del cableado estructurado.

3.5.1.1.1 Cableado Horizontal

- La necesidad de adición de puntos de red en varios departamentos de la institución debe ser validada en base al levantamiento de información realizado, con lo cual se brinde el servicio de red requerido por los usuarios.
- Para la ampliación del cableado horizontal se debe tener en cuenta el crecimiento estimado de la red, de manera que se brinde un servicio de red completo a todos los usuarios, tanto en la actualidad como en el futuro.
- Las nuevas conexiones de red no deben sobrepasar las distancias permitidas por la norma, además éstas deben seguir las rutas predefinidas y cumplir las demás especificaciones de las normas de cableado estructurado.
- Se debe realizar una reorganización de cables de red y cables eléctricos en las bandejas de distribución, separándolos físicamente los unos de los otros para evitar la interferencia electromagnética entre ellos.
- Todas las conexiones realizadas deben estar debidamente documentadas y etiquetadas de manera que permitan una clara identificación de las mismas. Así también se debe tener en cuenta que la etiquetación realizada en la institución debe permitir una fácil identificación respecto al servicio prestado y su ubicación; mediante el levantamiento de red realizado se ha determinado que el etiquetado utilizado no es el más adecuado, por lo cual se sugiere que se realice una nueva identificación y etiquetación de los puntos de red, además debe tenerse en cuenta que todos los puntos que se han añadido cuentan con una etiquetación no adecuada o simplemente no la tienen.

Propuesta de una nueva etiquetación

Los parámetros a tomarse en cuenta para la realización de una nueva identificación de los puntos de red en la institución son:

- *Bloque:*

Permite una fácil identificación del bloque al cual se brinde el servicio de red.

Tabla 16. Nomenclatura utilizada para los bloques

Bloque 1	B1
Bloque 2	B2
Bloque 3	B3
Bloque 4	B4
Bloque 5	B5
Bloque 6	B6
Bloque 7	B7

Fuente: Nancy Yolanda Ramón I.

- *Tipo de servicio (Tipo):*

Permite determinar el tipo de servicio prestado sea de voz o de datos.

Tabla 17. Nomenclatura utilizada para el tipo de servicio

Voz	V
Datos	D

Fuente: Nancy Yolanda Ramón I.

- *Número de Patch Panel (#PP):*

Permite identificar el patch panel en el cual se encuentra conectado el punto de red.

Tabla 18. Nomenclatura utilizada para el número de PP

PP. Uno	*1*
PP. Dos	*2*
PP. Tres	*3*

Fuente: Nancy Yolanda Ramón I.

- *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:

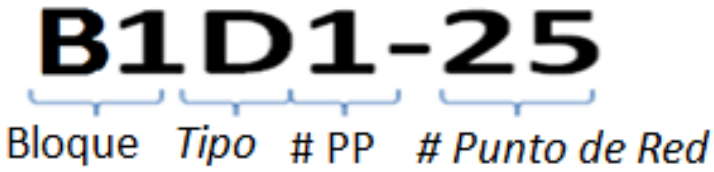


Figura 49. Ejemplo de propuesta de etiquetación

Fuente: Nancy Yolanda Ramón I.

Esta nueva etiquetación permitirá 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.

3.5.1.1.2 Cableado Vertical

- Del estudio realizado se ha verificado que dos de los bloques del edificio cuentan con backbone principal de cable UTP; considerando que por este canal se maneja gran cantidad de tráfico perteneciente a los usuarios de cada uno de los bloques, es importante asegurar que no existan cuellos de botella en la red, por lo cual es recomendable que se remplace estos enlaces de cable UTP por enlaces de fibra óptica, teniendo en cuenta que el equipamiento existente entre ellos lo soporta, de manera que se asegure conexiones a Gigabit.
- Para asegurar la disponibilidad de la red es necesario que se instale cableado de backup para lo cual se podría considerar dos opciones, una en la cual se utilice otros enlaces de fibra óptica, ó la utilización de cableado par trenzado UTP Cat 6a.

De instalarse enlaces de fibra óptica se aseguraría dos rutas que brinden conexiones a Gigabit Ethernet, sin embargo el instalar enlaces de cable UTP constituye una solución más económica y factible considerando que estos enlaces se los utilizaría netamente como backup.

- Así también como se recomendó en el capitulo anterior es necesario que la fibra óptica cuente con protección, de manera que se evite que se produzcan fallos en la misma debido a la mala manipulación, además se debe tener en cuenta las normas de cableado estructurado para tender las mismas junto con su respectiva etiquetación.

3.5.1.1.3 Cuarto de Telecomunicaciones

- Es importante considerar que para una mejor administración de la red, ésta debe contar con una debida organización por lo cual es necesario que todos los puntos de red lleguen hacia su respectivo patch panel para su distribución.
- Se debe eliminar los puntos de red que se encuentran utilizando jack como extensión hasta llegar a patch panel, ya que esto además de que no está permitido por las normas de cableado estructurado también disminuye el rendimiento de la misma y aumenta los puntos de falla.
- Es importante que todos los puntos de red instalados cumplan con las normas de cableado estructurado respetando la distancia hacia las tomas eléctricas, también es necesario que se separe el cableado de datos del cableado eléctrico, para evitar problemas de interferencia electromagnética. De igual forma las luminarias instaladas en los cuartos de telecomunicaciones deben mantener una adecuada separación de los rack de comunicaciones debido a la emisión de campo electromagnético que estas producen.
- A lo largo de la distribución del cableado estructurado se recomienda que se utilicen los debidos accesorios para su correcta instalación, evitando ángulos y tensiones inadecuadas en los enlaces de conexión.

3.5.1.1.4 Data Center

Es necesario que se tenga un especial cuidado con el cumplimiento de las normas de cableado estructurado en este cuarto, ya que el mismo constituye un punto crítico en la red, tomando en cuenta algunos criterios básicos como:

- Es importante que se cuente con red eléctrica de respaldo de manera que no se tenga cortes de servicio por falla del suministro eléctrico.
- Se debe mantener un control sobre los elementos que constituyen el cableado de datos contando con los respectivos manejadores de cable y accesorios; así también es importante el uso adecuado de los patch panel que permitan una correcta administración de este cuarto.
- De igual forma para asegurar la conexión es preciso utilizar patch cords y cables de fibra óptica certificados lo cuales garanticen la conexión hacia el equipamiento activo y la zona de servidores.
- Se debe tener en cuenta realizar mantenimientos periódicos al sistema de aire acondicionado de manera que se mantenga una temperatura adecuada en el Data Center.

3.5.2 POLÍTICAS DE ADMINISTRACIÓN DE LA PARTE ACTIVA

Dentro de las políticas de seguridad para la parte activa se debe tener en cuenta lo siguiente:

- El acceso remoto debe ser encriptado utilizando protocolo SSH versión 2 de preferencia, los accesos vía telnet deben ser suspendidos definitivamente y se deben definir los equipos en la red que están autorizados a acceder a la administración de los mismos.
- Las interfaces de administración web deben ser deshabilitadas de forma definitiva o debe controlarse el acceso a las mismas únicamente desde los equipos de los administradores de red.
- Los administradores de red deben cambiar periódicamente las contraseñas de los equipos de parte activa, utilizando contraseñas seguras y encriptadas.

- En los documentos de configuración debe explicarse detalladamente los comandos aplicados y su funcionalidad.
- La actualización de los IOS debe realizarse de forma periódica y debe tomarse en cuenta como un parámetro a definir periódicamente en el mantenimiento de los mismos.
- Se deben crear procesos y procedimientos que describan las acciones y eventos que se deban realizar en caso de que no se encuentre el personal de administración de la red. Además si se presentan nuevos eventos es necesario actualizar siempre estos procedimientos.
- Es importante tener una bitácora en la cual se registren todos los eventos suscitados en la red.
- Es necesario hacer el levantamiento de información relacionada a componentes de hardware y software de los equipos y dispositivos conectados a la red de datos de la Institución de manera que se pueda controlar el cambio y uso de los recursos existentes.
- Se debe aplicar una reingeniería según estándares internacionales para el mejoramiento del performance de dicha red, mediante la redistribución del equipamiento, creación de backups a todo nivel, incluidas las redundancias físicas; además se deben aplicar protocolos como Spanning Tree según los requerimientos para evitar que se produzcan lazos en la red.
- Se debe reestructurar la segmentación del tráfico para el mejor rendimiento de los departamentos que pertenecen a la red de la institución.
- Se recomienda implementar software libre de monitoreo y gestión que permita ver las características en tiempo real de la red, así como la disponibilidad del servicio de red.

3.5.3 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.

En la figura se observa el modelo general que se propone implementar en la red de la Institución.

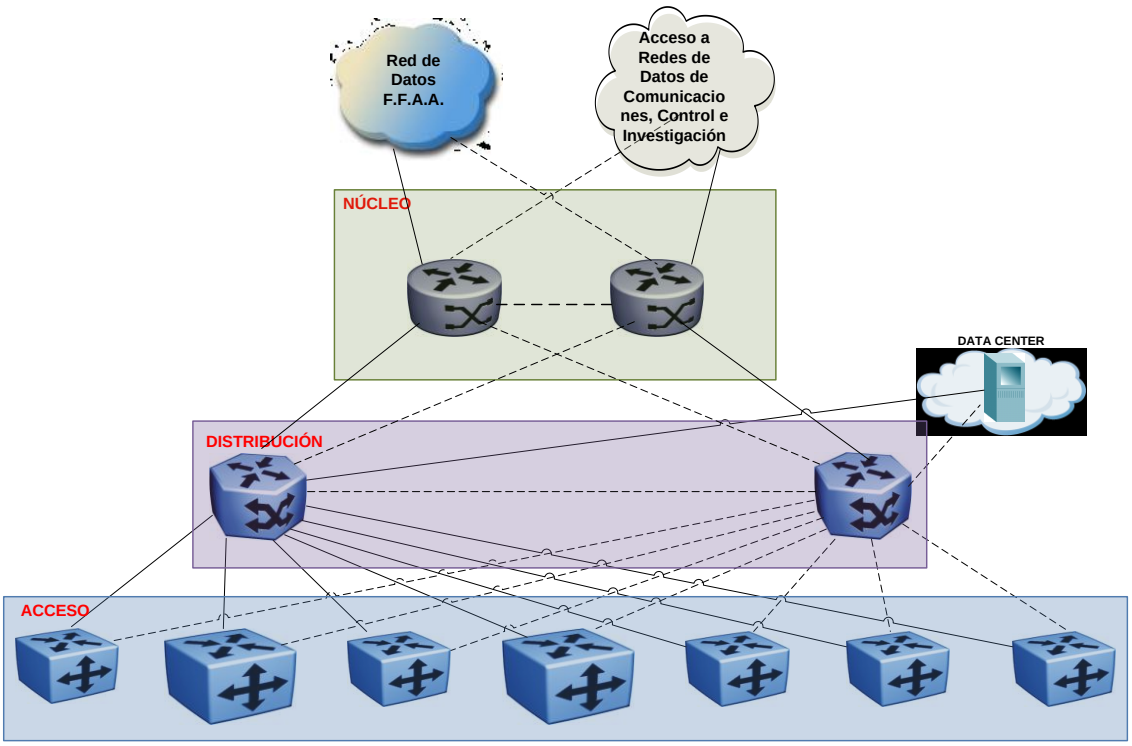


Figura 50. Modelo general de la red de datos

Fuente: Nancy Yolanda Ramón I.

En la figura se observa de forma general el modelo de red planteado para la institución, en base al cual para cada una de las capas se definirá 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 switches del 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 han considerado 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 que se proponen brindan disponibilidad a la red, por lo cual se deben duplicar las conexiones y el equipamiento. Se ha considerado las medidas del diámetro de la red en función de la mayor cantidad de equipamiento, la misma que es de tres.

3.5.3.1 Nivel de núcleo

Este nivel es el backbone principal para la red de datos de la Institución y para los respectivos entes del MIDENA, así también, este nivel manejará todo el tráfico proveniente de los equipos de la capa de distribución de la red 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 en la red.

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.

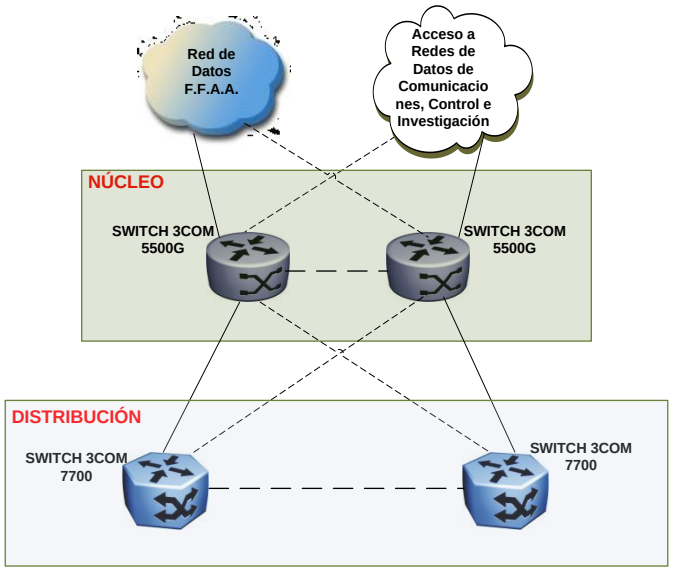


Figura 51. Nivel de núcleo del modelo de red

Fuente: Nancy Yolanda Ramón I.

A este nivel se utilizará como equipamiento activo los switch 3com serie 5500G los cuales entre sus características más destacadas para éste estudio, cuenta con puertos Gigabit Ethernet, maneja puertos para estaqueo, presenta funciones de L2 y L3, manejo de VLAN, MSTP, STP y agregado de enlace.

3.5.3.1.1 Consideraciones de diseño

- Es importante tener en cuenta que debido a que en este nivel se manejarán todos los enlaces hacia la red de datos, las redundancias físicas de los enlaces deben contar con caminos diferentes, de manera que se evite riesgos debido a fallas en la trayectoria asegurando su disponibilidad. Cumpliendo con el modelo de red diseñado, todos los entes del Ministerio de Defensa Nacional deben adaptarse a su diseño, de manera que éstos cuenten con el servicio y las ventajas de pertenecer a la red de datos, permitiéndoles acceder a todas las aplicaciones manejadas de forma

interna por una red independiente sin consumir el ancho de banda asignado para la navegación, además sin depender de un canal asignado para navegación para contar con el acceso a la red de Fuerzas Armadas y de una forma segura.

- Así también debido a que desde el equipamiento de esta capa de red se manejará todo el tráfico generado para la red de datos se debe manejar un diseño con segmentación a nivel lógico para lo cual se precisa la configuración de VLAN, de forma que se controle el tráfico generado por cada una de las fuerzas adscritas a la misma.

Para cada uno de los entes del Ministerio de Defensa se utilizará una VLAN diferente con la cual además de controlar el tráfico generado entre cada uno de los entes se brindará seguridad a los mismos.

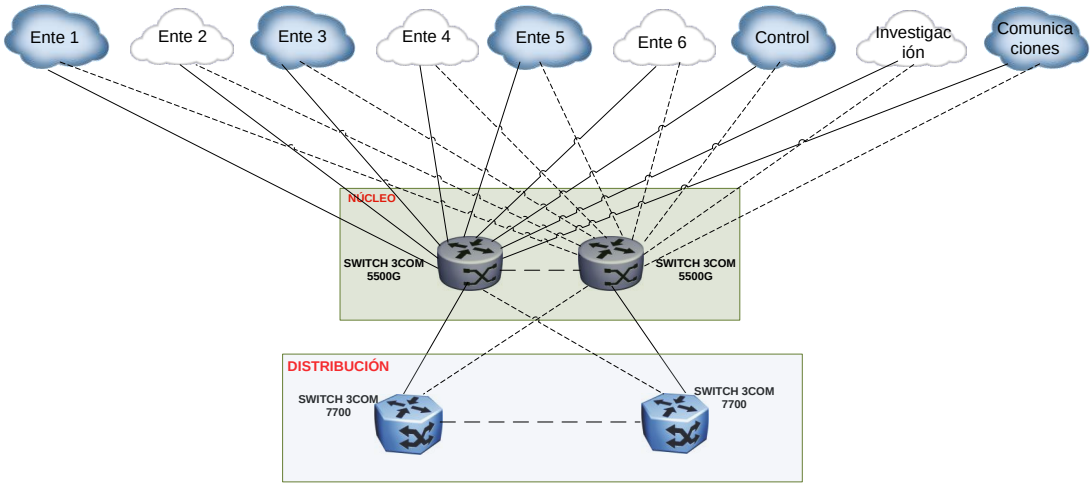


Figura 52. Nivel de núcleo extendido del modelo de red

Fuente: Nancy Yolanda Ramón I.

- Debido a que el diseño de red planteado es redundante es necesario además utilizar MSTP (Protocolo Múltiple SpanningTree) para evitar tormentas de broadcast y un excesivo consumo de ancho de banda.
- Aunque al momento se cuenta con disponibilidad de puertos en el equipamiento activo, de necesitarse puertos adicionales los equipos utilizados brindan la ventaja de permitir apilar switches de forma que el performance de la red no se vea afectado.

- Así también debido a que el enrutamiento de tráfico utilizado para la red de datos es dinámico, y como estándar de las Fuerzas Armadas se utiliza enrutamiento OSPF, cada uno de los entes del Ministerio de Defensa debe utilizar un área diferente en función de la siguiente distribución:

Tabla 19. Distribución de áreas para enrutamiento dinámico OSPF

Nombre	Número de Área
Ente 1	Área 1
Ente 2	Área 2
Ente 3	Área 3
Ente 4	Área 0
Ente 5	Área 4
Ente 6	Área 5
Control	Área 6
Investigación	Área 7
Comunicaciones	Área 8

Fuente: Nancy Yolanda Ramón I.

3.4.3.2 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.

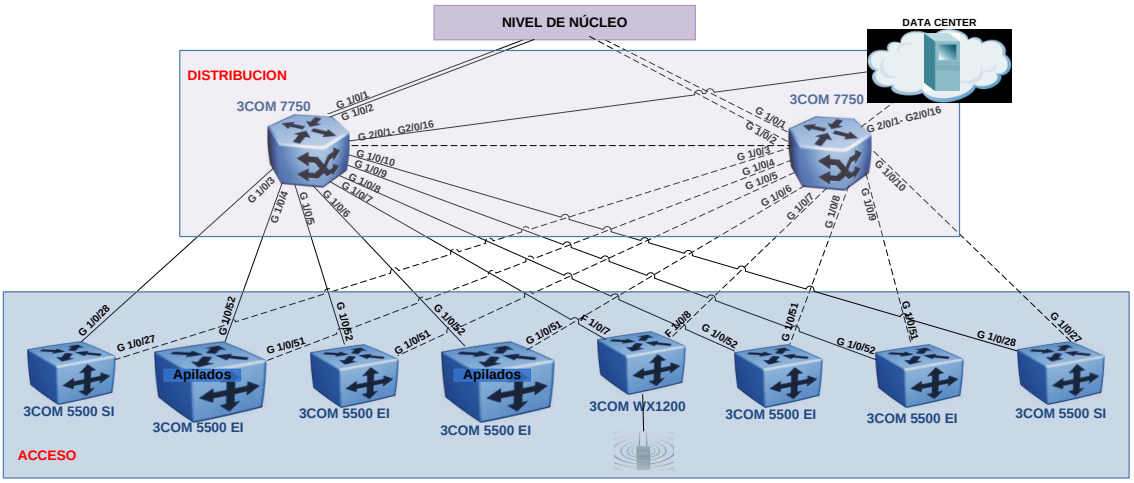


Figura 53. Nivel de distribución del modelo de red

Fuente: Nancy Yolanda Ramón I.

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. La institución cuenta con equipamiento marca 3Com de la serie 7700 el cual es un switch capa 3 modular, éste se adapta de forma apropiada al modelo de red planteado, dado que entre sus principales características tiene soporte de L2 y L3, soporte de switching 10Gigabit, Gigabit y Fast Ethernet, soporte de PoE, soporte de ACL, MSTP, SNMPv3, soporte de agregados de enlace y manejo de una plataforma de chasis, permitiendo agregar nuevos módulos de requerir crecimiento a nivel de puntos de red.

3.4.3.2.1 Consideraciones de diseño

- El switch 3Com serie 7700 manejará los enlaces de conexión con los bloques de la institución, además los enlaces de conexión hacia los servidores de aplicación; así también 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.
- Además a este nivel se realizará enrutamiento, el cual se ha establecido OSPF como estándar a nivel de la red de Fuerzas Armadas manejando el área asignada a cada una de las fuerzas. En el caso de la institución en estudio se manejará el área 0.

- Debido a que éste equipo será el backbone de la red interna es recomendable usar un switch adicional de backup para asegurar el rendimiento de la red y evitar caídas de servicio en la red interna de la institución; es importante contar con redundancia tanto a nivel del equipamiento activo como a nivel del backbone asegurando la conexión con los equipos de la capa de acceso como con la capa de núcleo, para la cual como se mencionó anteriormente es posible realizar los enlaces de backup con fibra óptica o con cableado UTP según las necesidades y recursos de la Institución.

3.5.3.2.2 Requerimientos:

- En base al estudio realizado en el capítulo anterior y teniendo en cuenta el crecimiento de la red se requiere la adquisición de un módulo para el switch 3com serie 7700 dado que al momento este equipo tiene poca disponibilidad de puertos.
- Adicionalmente para contar con disponibilidad en la red es necesario contar con el equipamiento para backup el cual debe poseer características similares al equipo de distribución principal de manera que este equipo ofrezca las mismas funcionalidades de red como las que se menciona a continuación:
    - **Soporte de Capa 3**.
    - **Políticas de seguridad y ACL:** soporte de seguridad a nivel de puerto y manejo de listas de acceso para permitir o negar el tráfico generado en la red.
    - **QoS:** en caso de que se pretenda usar telefonía IP o IPTv en futuras aplicaciones y se tenga que priorizar el envío del tráfico por la red.
    - **Alta tasa de envío:** con un alto backplane soportando aplicaciones de red exigentes (disponibilidad del 99,999%) y cumpliendo con los requerimientos.
    - **Gigabit Ethernet y 10 Gigabit Ethernet:** para futuras aplicaciones y conforme el crecimiento de la red se recomienda realizar un upgrate a los equipos y aumentar módulos de 10 Gigabit Ethernet.

- **Componentes redundantes:** por lo que ya se ha mencionado y justificado anteriormente es necesario tener una redundancia de equipos y de conexiones.
- **Agregado de enlaces**: por medio de este método es posible aumentar el rendimiento del equipamiento activo.
- **Velocidad de cable:** definida por la capa física de red.

- Para el backup a nivel de conexiones de red es necesario el tendido de cable de fibra óptica o en su defecto cable UTP como cableado de backup entre equipamiento activo, con lo que se cumpla el modelo de red establecido, así también es necesario que se valide que todos los enlaces de conexión principales de fibra óptica se encuentren operando satisfactoriamente para evitar pérdidas de paquetes y reducción del rendimiento en la red.
- Teniendo en cuenta que el modelo manejará enlaces redundantes es necesario que se maneje MSTP para evitar tormentas de broadcast en la red.

3.5.3.3 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, cámaras IP, entre otros; así también en este nivel se controlan los equipos que se conectan a la red.

Figura 54. Nivel de acceso del modelo de red

Fuente: Nancy Yolanda Ramón I.

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
    - Dirección MAC y dirección IP.
- **PoE:** de ser necesario se puede considerar que los switches soporten Power Over Ethernet (PoE). Se debe tener en cuenta que el switch 3Com WX1200 soporta PoE, el cual al momento no se encuentra conectado de manera óptima, por lo que se recomienda que la conexión con la capa de distribución se realice por los puertos 7 y 8 (con redundancia) que son autonegociables y las salidas para los AP o futuras implementaciones de una red wireless se utilicen los puertos del 1 al 6. Además se recomienda para este equipo la adquisición del 3Com Wireless LAN Controller WX4400, que permitiría crear una red inalámbrica, administrar y gestionar la misma.

- **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).

3.5.3.3.1 Consideraciones de diseño

- Dentro del diseño se ha considerado la segmentación a nivel lógico de la red. Con el levantamiento de información realizado previamente, se ha verificado que los usuarios se encuentran agrupados en función de bloques y más no en base a funciones y los recursos que comparten, esto ha conllevado problemas relacionados a la densidad del equipamiento activo y un elevado flujo de tráfico. Esta distribución no permite la movilidad de los usuarios en función de la VLAN sino más bien los usuarios deben adaptarse hacia el bloque al cual son redirigidos ocasionando cambios bruscos en la red y a nivel de usuario final; dificultando la escalabilidad a nivel de red.
- Teniendo en cuenta que para tener un control de la infraestructura de red, es importante asegurar que cada usuario tenga una dirección IP asignada, la misma que no sea cambiada sin previa autorización; para subsanar los posibles inconvenientes en la gestión y administración de la red se utilizará ***Access management*** a nivel de puerto de manera que se restringa el uso de la red a un determinado usuario haciendo referencia a la dirección MAC y dirección IP del equipo; si uno de los dos parámetros falla el equipo no podrá conectarse a la red.
- 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.
    - 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.

Contando con la información actualizada sobre el estado de la red, de existir problemas se podría identificar visualmente los potenciales cuellos de botella al evaluar el tráfico u otros problemas asociados en función de las áreas de servicio permitiendo brindar una solución oportuna sin afectar a toda la red.

- El modelo actual de red tiene switches en configuración en cascada debido a la demanda de puertos y con el objetivo de brindar conectividad, sin embargo esto reduce el rendimiento de la red.

  Una solución para evitar los switches en cascada es aplicar apilamiento, éste tipo de solución permite:

  - Operación con efectividad como un único switch más grande.
  - El uso de conexiones cruzadas de manera que la red pueda recuperarse rápidamente si falla un único switch.
  - Utilización de un puerto especial para las interconexiones de forma que no se utilice puertos de línea para las conexiones inter-switches.
  - Velocidades más rápidas de conexión de switches.
  - Convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular.

  El Apilamiento es una tecnología propietaria de 3Com denominada XRN. La tecnología XRN se administra como una sola unidad, con toda la conmutación y el enrutamiento distribuido entre los múltiples dispositivos (switches).

Las ventajas que se obtiene al utilizar este tipo de tecnología son:

- **Alto rendimiento:** Una red que usa tecnología XRN puede usar múltiples switches Gigabit Capa 3 para escalar el rendimiento y la densidad de los puertos. La tecnología XRN también soporta Agregación de Enlaces (Link Aggregation) por todo el Fabric Distribuido, incrementando tanto el rendimiento como la disponibilidad.

- **Escalabilidad**: Si existe una ampliación de la cantidad de puertos en cualquier bloque se puede aumentar unidades adicionales sin reducir el rendimiento de la red.

- **Simplicidad de administración:** Fácil administración debido a que los switches apilados son administrados como una sola unidad, con una sola dirección IP, una sola configuración y sus configuraciones son sencillas de realizarlas.

- **Flexibilidad:** Varios tipos de switches Gigabit Capa 3 de 3Com soportan la tecnología XRN. Esto brinda la capacidad de mezclar y combinar diferentes medios y configuraciones de puertos en una sola unidad.

Como requerimiento para apilar switches 3Com debe tenerse en cuenta que utilicen la misma versión de Sistema Operativo y además usen el mismo *sysname*. El número máximo de switch que pueden apilarse es 8.

3.5.4 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.

3.5.4.1 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.

La asignación de la VLAN para cada ente involucrado se observa en la tabla 20, junto al direccionamiento IP aplicado.

Tabla 20. Direccionamiento IP para enlaces de la red de datos

Descripción	VLAN	Nombre	Direccionamiento IP
Ente1	Vlan 2	Ente1	10.51.10.24/29
Ente2	Vlan 3	Ente2	10.51.10.32/29
Ente3	Vlan 4	Ente3	10.51.10.40/29
Ente4	Vlan 5	Ente4	10.51.10.48/29
Ente5	Vlan 6	Ente5	10.51.11.56/29
Ente6	Vlan 7	Ente6	10.51.11.64/29
Control	Vlan 8	Ctrl	10.51.11.72/29
Investigación	Vlan 9	Inves	10.51.11.80/29
Comunicaciones	Vlan 10	Comu	10.51.11.88/29

Fuente: Nancy Yolanda Ramón I.

La configuración de las VLAN se realizará a nivel de los switches 5500G del nivel de núcleo, en los cuales se encuentran conectados los enlaces hacia cada uno de los entes respectivos, así también los enlaces redundantes que aseguran su disponibilidad.

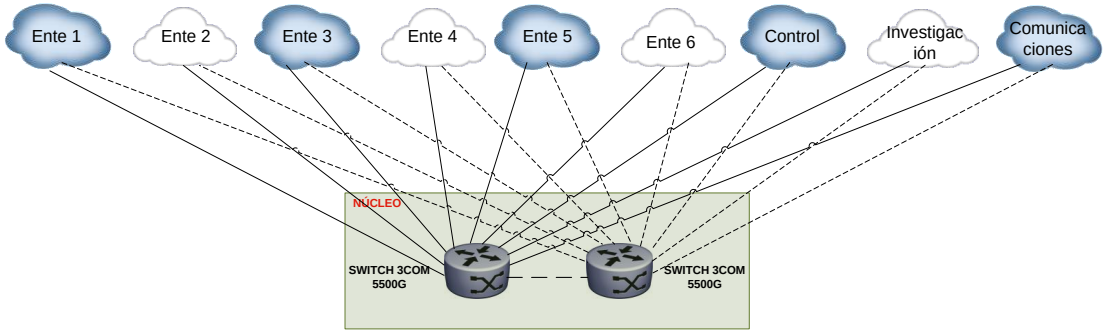


Figura 55. Esquema gráfico segmentación para el nivel de núcleo

Fuente: Nancy Yolanda Ramón I.

3.5.4.2 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 ha segmentado la red en grupos o VLAN. Su distribución de manera gráfica se puede observar en la figura 56, en la cual se ilustra cada una de las subredes con un color diferente; además se puede notar que algunas de las subredes pertenecen a más de un bloque lo cual indica la asociación de los usuarios independiente de su ubicación física en la red.

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.

En el Anexo 4 "*Direccionamiento IP basado en VLAN*" se puede observar la distribución de los usuarios en base a la VLAN designada.

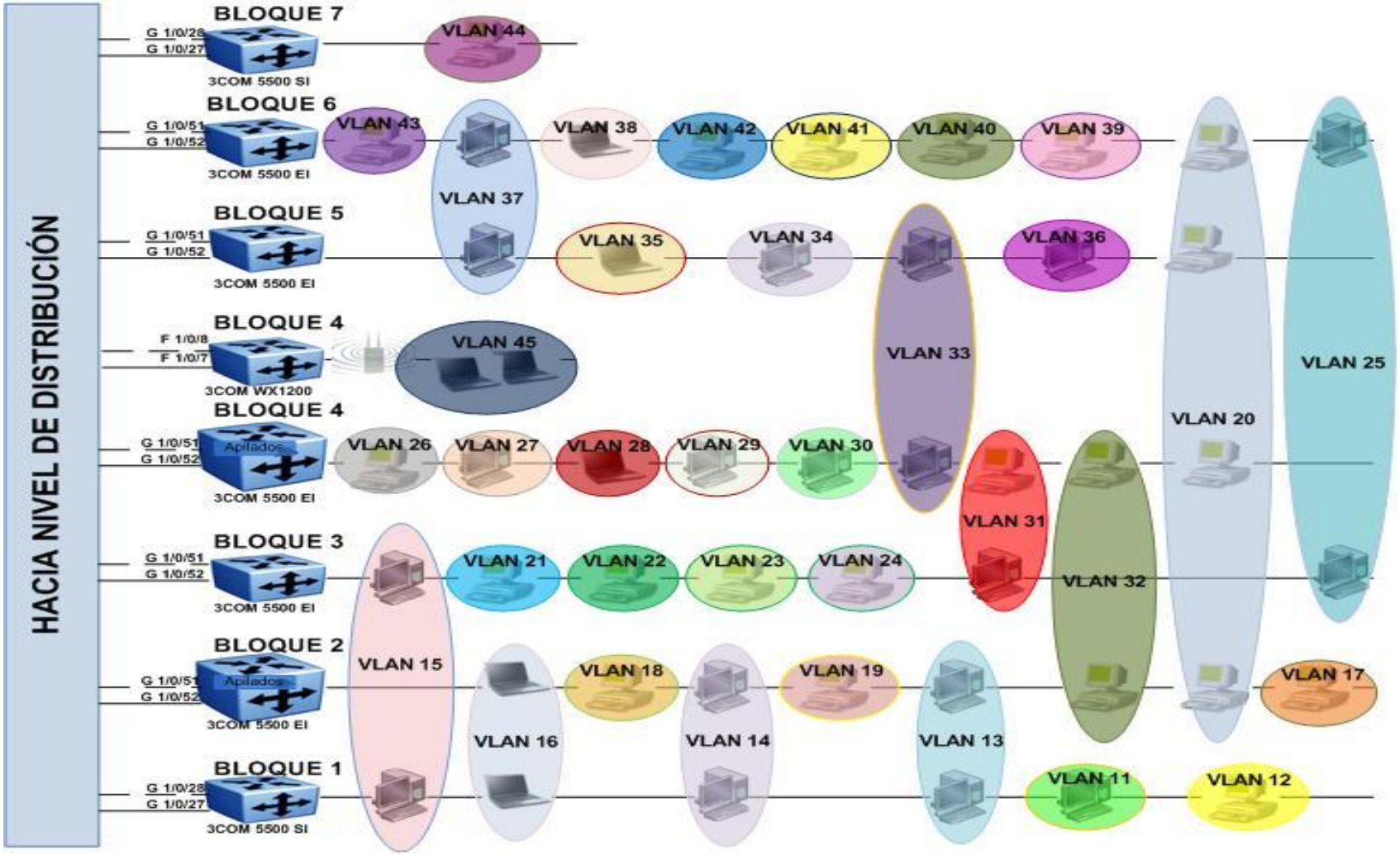


Figura 56. Propuesta gráfica de la segmentación para el nivel de acceso

Fuente: Nancy Yolanda Ramón I.

La asignación del direccionamiento IP para cada una de las VLAN está basado en un direccionamiento eficiente VLSM, el cual permite la asignación utilizando una máscara variable optimizando el uso de la redes determinadas para la institución, la asignación del direccionamiento se lo ha realizado comenzando con los grupos con mayor densidad de usuarios, hasta terminar con los grupos con menor cantidad de usuarios.

Teniendo en cuenta las redes asignadas hacia la institución se las ha utilizado de la siguiente manera:

- 10.10.20.0 - utilizada para la red de servidores y equipos.
- 10.10.19.0
- 10.10.18.0
- 10.10.17.0 - redes disponibles
- 10.10.16.0
- 10.10.15.0
- 10.10.14.0
- 10.10.13.0 - utilizada para la red wireless.
- 10.10.12.0
- 10.10.11.0 - utilizadas para la segmentación de la red interna.
- 10.10.10.0
- 10.10.9.0

En la tabla 21 se puede observar la distribución del direccionamiento IP aplicado en función de cada una de las VLAN creadas, junto con su respectiva máscara de red, puerta de enlace y ubicación.

Tabla 21. Direccionamiento IP para el nivel de acceso

VLAN	DEPENDENCIA	NOMBRE	#PUNTOS DE RED	#PUNTOS + 50%	MÁSCARA RED	DIRECCIONAMIENTO IP	GATEWAY	LOCALIZACIÓN BLOQUES
Vlan 1	Servidores y Equipos	SRVEQU	50		/25	10.10.20.0 - 10.10.20.127	10.10.20.1	DATACENTER
Vlan 3	Centro de Conmutación	CCONMUTA	2		/29	10.51.10.48 - 10.51.10.55		DATACENTER
Vlan 11	Unidad Ejecutora	UNIEJE	9	14	/27	10.10.10.224 - 10.10.10.255	10.10.10.225	B1
Vlan 12	Departamento de Sistemas/Comunicaciones	COMU	5	8	/28	10.10.11.160 - 10.10.11.175	10.10.11.161	B1
Vlan 13	Dirección Administrativa/Seguridad	SEGU	5	8	/28	10.10.11.176 - 10.10.11.191	10.10.11.177	B1 - B2
Vlan 14	Cuarto de Control	CCTRL	6	9	/28	10.10.11.96 - 10.10.11.111	10.10.11.97	B1 - B2
Vlan 15	Dirección de Logística	DIRLOGI	16	24	/27	10.10.9.192 - 10.10.9.223	10.10.9.193	B1 - B3
Vlan 16	Departamento de Control	DEPCON	13	20	/27	10.10.10.32 - 10.10.10.63	10.10.10.33	B1 - B2
Vlan 17	Dirección de Personal	DIRPER1	14	21	/27	10.10.10.0 - 10.10.10.31	10.10.10.1	B2
Vlan 18	Dirección de Personal	DIRPER2	11	17	/27	10.10.10.128 - 10.10.10.159	10.10.10.129	B2
Vlan 19	Asuntos Internacionales	ASUINT	5	8	/28	10.10.11.192 - 10.10.11.207	10.10.11.193	B2
Vlan 20	Salas de Reuniones	SREU	50		/26	10.10.9.0 - 10.10.9.63	10.10.9.1	B2 - B4 -B5 - B6
Vlan 21	Cuartel General	CGRAL	4	6	/28	10.10.12.32 - 10.10.12.47	10.10.12.33	B3
Vlan 22	Departamento de Ingeniería	DEPING	8	12	/28	10.10.11.32 - 10.10.11.47	10.10.11.33	B3
Vlan 23	Departamento de Contratación Pública	CONPUB	5	8	/28	10.10.11.208 - 10.10.11.223	10.10.11.209	B3

Vlan 24	Dirección de Sanidad	SANIDAD	15	23	/27	10.10.9.224 - 10.10.9.255	10.10.9.225	B3
Vlan 25	Departamento de Evaluación y Control	EVACTRL	6	9	/28	10.10.11.112 - 10.10.11.127	10.10.11.113	B3 - B6
Vlan 26	Dirección de Telecomunicaciones	DIRTEL	18	27	/27	10.10.9.160 - 10.10.9.191	10.10.9.161	B4
Vlan 27	Dirección de Sistemas	DIRSIST1	12	18	/27	10.10.10.96 - 10.10.10.127	10.10.10.97	B4
Vlan 28	Dirección de Sistemas	DIRSIST2	13	20	/27	10.10.10.64 - 10.10.10.95	10.10.10.65	B4
Vlan 29	Dirección de Sistemas	DIRSIST3	7	11	/28	10.10.11.64 - 10.10.11.79	10.10.11.65	B4
Vlan 30	Dirección de Sistemas	ADMIN	3	5	/29	10.10.12.64 - 10.10.12.71	10.10.12.65	B4
Vlan 31	Dirección Administrativa	DIRADM1	8	12	/28	10.10.11.48 -10.10.11.63	10.10.11.49	B3 - B4
Vlan 32	Dirección Administrativa	DIRADM2	19	29	/27	10.10.9.128 - 10.10.9.159	10.10.9.129	B2 - B4
Vlan 33	Dependencia Jurídica	JURIDICO	7	11	/28	10.10.11.80 - 10.10.11.95	10.10.11.81	B4 - B5
Vlan 34	Jefatura	JEFATURA1	10	15	/27	10.10.10.192 - 10.10.10.223	10.10.10.193	B5
Vlan 35	Jefatura	JEFATURA2	5	8	/28	10.10.11.224 - 10.10.11.239	10.10.11.225	B5
Vlan 36	Dirección de Intereses Nacionales	INTNAC	5	8	/28	10.10.11.240 - 10.10.11.255	10.10.11.241	B5
Vlan 37	Dirección de Desarrollo Institucional	DESAINST	20	30	/26	10.10.9.64 - 10.10.9.127	10.10.9.65	B5 - B6
Vlan 38	Dirección de Operaciones	DIROPE	5	8	/28	10.10.12.0 - 10.10.12.15	10.10.12.1	B6
Vlan 39	Cooperación Interinstitucional	COOPINTER	6	9	/28	10.10.11.128 -10.10.11.143	10.10.11.129	B6

Vlan 40	Dirección de Doctrina	DOCTRINA	5	8	/28	10.10.12.16 - 10.10.12.31	10.10.12.17	B6
Vlan 41	Dirección de Planes y Ordenes	PLANORD	11	17	/27	10.10.10.160 - 10.10.10.191	10.10.10.161	B6
Vlan 42	Federación Deportiva	FEDDEP	6	9	/28	10.10.11.144 - 10.10.11.159	10.10.11.145	B6
Vlan 43	Dirección de Comunicación Social	COMSOC	4	6	/28	10.10.12.48 -10.10.12.63	10.10.12.49	B6
Vlan 44	Dirección de Investigaciones	DIRINV	9	14	/27	10.10.11.0 - 10.10.11.31	10.10.11.1	B7
Vlan 45	Red Wireless	WIRELESS			/24	10.10.13.0 - 10.10.13.255	10.10.13.1	B4

Fuente: Nancy Yolanda Ramón I.

Dentro de la distribución de VLAN se pueden diferenciar seis clasificaciones de la siguiente manera:

- **VLAN de conexión con el Centro de Conmutación (CCONMUTA):** es utilizada para la interconexión con el Centro de Conmutación y la Institución, por medio de este enlace se asegura la comunicación con la red de datos del Ministerio de Defensa.

- **VLAN de Servidores y Equipos (SRVEQU):** es utilizada para el direccionamiento IP de la granja de servidores de aplicación de la Institución y el equipamiento activo.

- **VLAN de Administración (ADMIN):** subred perteneciente netamente a los administradores de red, únicamente los usuarios contenidos en esta subred tienen acceso a la administración del equipamiento activo.

- **VLAN de Salas de Reuniones (SREU**): esta subred contiene las salas de reuniones de cada uno de los diferentes bloques, en las mismas que a más de realizarse reuniones de las diferentes direcciones, se realizan capacitaciones por lo cual estas deben estar aisladas del resto de la red.

- **VLAN para la red Wireless (WIRELESS):** subred utilizada para la red Wireless de la Institución, la misma que por motivos de seguridad deberá permanecer aislada del resto de la red.

- El resto de las VLAN asignadas pertenecen a los diferentes grupos de usuarios.

La declaración de las VLAN asignadas para el edificio se realizará en el switch 3Com serie 7700, el mismo que como se explicó realizará el enrutamiento INTERVLAN; a nivel de acceso se configurará las VLAN en los switch 3com de la serie 5500, los cuales brindarán la conexión hacia el usuario final, cada uno de los puertos serán configurados según la VLAN asociada al usuario.

3.5.4.2 Listas de Control de Acceso

Una lista de control de acceso (ACL) es utilizada para identificar flujos de tráfico, la cual al filtrar los paquetes de datos permite o deniega el tráfico cursante, de manera que se limite el tráfico en la porción de red requerida.

Una ACL puede clasificar los paquetes basándose en una serie de condiciones como por ejemplo: en función de una dirección origen, dirección de destino, protocolo o puertos.

Las listas de control de acceso en la tecnología 3Com están clasificadas en cuatro grupos:

- ACL Básica (numeradas del 2000 a 2999): basadas en la dirección origen.
- ACL Avanzada (numeradas del 3000 a 3999): basadas en la dirección de origen, dirección de destino, protocolo, número de puerto y otros parámetros específicos.
- ACL de capa 2 (numeradas del 4000 a 4999): basadas en campos de la cabecera de protocolo de capa 2, como dirección MAC origen, dirección MAC destino, prioridad 802.1p, y el tipo de protocolo de capa enlace.
- ACL definida por el usuario (numeradas del 5000 a 5999): basadas en información personalizada de los encabezados de protocolo.

Dentro de la clasificación de las listas de acceso las opciones más utilizadas son las ACL básicas y ACL avanzadas en los equipos de nivel de acceso.

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 (2800 y 2900):** utilizadas para limitar el tráfico generado por las diferentes redes.

- **Lista de acceso avanzada (3800):** utilizadas para limitar la administración del equipamiento activo a la VLAN de Administradores.

Estas listas de control de acceso serán configuradas en los switch 3com de la serie 5500 en el nivel de acceso.

3.5.4.2.1 Lista de control de acceso básica 2800

La función de la ACL 2800 será negar el tráfico de todas las redes internas, utilizadas en el edificio. Las reglas de la lista de acceso deben ser configuradas en los puertos trunk de cada uno de los switch de bloque, ya que por medio de este puerto se encamina todo el tráfico generado.

La lista de acceso 2800 es una lista de acceso básica ya que netamente será la encargada de negar el tráfico generado en la red.

Con las reglas aplicadas en la lista de acceso 2800 en primera instancia se encuentra negado todo el tráfico proveniente de las redes asignadas. De no crear alguna regla para permitir el tráfico en alguna de las subredes, las máquinas de los usuarios no tendrían conexión con ninguna de las demás subredes, ni con los miembros de la misma subred.

3.5.4.2.2 Lista de acceso 3800

La función de la lista de acceso 3800 será permitir que se genere tráfico entre los miembros de una VLAN.

De igual forma que la lista de acceso 2800, las reglas pertenecientes a la lista de acceso 3800 se las configurará en los puertos trunk de cada uno de los switches de acceso.

A diferencia de las reglas de acceso 2800, estas deben ser configuradas dependiendo de su necesidad, es decir simplemente las subredes que estén configuradas en el switch, su asignación está dada en función de la regla asociada a cada una de las VLAN como se observa a continuación en la tabla 22:

Tabla 22. Asignación de ACL en función de la VLAN

VLAN	DEPENDENCIA	NOMBRE	NÚMERO ACL	LOCALIZACIÓN BLOQUES
Vlan 1	Servidores y Equipos	SRVEQU		DATACENTER
Vlan 3	Centro de Conmutación	CCONMUTA		DATACENTER
Vlan 11	Unidad Ejecutora	UNIEJE	Rule 1	B1
Vlan 12	Departamento de Sistemas/Comunic	COMU	Rule 2	B1
Vlan 13	Dirección Administrativa/Seguridad	SEGU	Rule 3	B1 - B2
Vlan 14	Cuarto de Control	CCTRL	Rule 4	B1 - B2
Vlan 15	Dirección de Logística	DIRLOGI	Rule 5	B1 - B3
Vlan 16	Departamento de Control	DEPCON	Rule 6	B1 - B2
Vlan 17	Dirección de Personal	DIRPER1	Rule 7	B2
Vlan 18	Dirección de Personal	DIRPER2	Rule 8	B2
Vlan 19	Asuntos Internacionales	ASUINT	Rule 9	B2
Vlan 20	Salas de Reuniones	SREU	Rule 10	B2 - B4 -B5 - B6
Vlan 21	Cuartel General	CGRAL	Rule 11	B3
Vlan 22	Departamento de Ingeniería	DEPING	Rule 12	B3
Vlan 23	Departamento de Contratación Pública	CONPUB	Rule 13	B3
Vlan 24	Dirección de Sanidad	SANIDAD	Rule 14	B3
Vlan 25	Departamento de Evaluación y Control	EVACTRL	Rule 15	B3 - B6
Vlan 26	Dirección de Telecomunicaciones	DIRTEL	Rule 16	B4
Vlan 27	Dirección de Sistemas	DIRSIST1	Rule 17	B4
Vlan 28	Dirección de Sistemas	DIRSIST2	Rule 18	B4
Vlan 29	Dirección de Sistemas	DIRSIST3	Rule 19	B4
Vlan 30	Dirección de Sistemas	ADMIN	Rule 20	B4
Vlan 31	Dirección Administrativa	DIRADM1	Rule 21	B3 - B4
Vlan 32	Dirección Administrativa	DIRADM2	Rule 22	B2 - B4
Vlan 33	Dependencia Jurídica	JURIDICO	Rule 23	B4 - B5
Vlan 34	Jefatura	JEFATURA1	Rule 24	B5
Vlan 35	Jefatura	JEFATURA2	Rule 25	B5
Vlan 36	Dirección de Intereses Nacionales	INTNAC	Rule 26	B5
Vlan 37	Dirección de Desarrollo Institucional	DESAINST	Rule 27	B5 - B6
Vlan 38	Dirección de Operaciones	DIROPE	Rule 28	B6

Vlan 39	Cooperación Interinstitucional	COOPINTER	Rule 29	B6
Vlan 40	Dirección de Doctrina	DOCTRINA	Rule 30	B6
Vlan 41	Dirección de Planes y Ordenes	PLANORD	Rule 31	B6
Vlan 42	Federación Deportiva	FEDDEP	Rule 32	B6
Vlan 43	Dirección de Comunicación Social	COMSOC	Rule 33	B6
Vlan 44	Dirección de Investigaciones	DIRINV	Rule 34	B7
Vlan 45	Red Wireless	WIRELESS	Rule 35	B4

Fuente: Nancy Yolanda Ramón I.

Adicionalmente a las reglas que permiten el tráfico entre los miembros de las VLAN, se debe crear una regla que permita el acceso a la Administración del equipamiento activo a la red de Administradores.

2.4.4.2.3 Lista de acceso básica 2900

Esta lista de acceso limitará el acceso remoto para la administración del equipamiento activo a la VLAN de los Administradores, a todas las demás redes se negará su acceso.

Esta lista de acceso debe ser configurada en la interface vty de cada switch.

3.5.5 MANEJO DE USUARIOS Y CONTRASEÑAS

Para la administración de los switches es importante definir los niveles de acceso para los usuarios, la tecnología 3Com cuenta con cuatro niveles:

- **Nivel 0 (Visit):** En este nivel se incluye comandos para realizar el diagnóstico de la red (como *ping* y *traceroute*), comandos para cambiar el idioma en la interfaz de usuario (*language-mode*) y el comando *telnet*. Este nivel no permite guardar los cambios de configuración.
- **Nivel 1 (Monitor):** Este nivel se permite comandos para monitoreo (display), obtener información y eventos del sistema (*debugging*) y realizar diagnósticos de las fallas de servicio. Este nivel tampoco permite guardar configuraciones.

- **Nivel 2 (Manager):** Este nivel permite usar comandos para enrutamiento y comandos de la capa de red, y se utilizan para proporcionar servicio de red directo al usuario. Este nivel permite guardar modificaciones y configuraciones. No permite crear usuarios.
- **Nivel 3 (Administrator):** Los comandos en este nivel son los que influyen en el funcionamiento básico del módulo de apoyo del sistema, que desempeña un papel de apoyo de los servicios. Los comandos en este nivel incluyen comandos del sistema de archivos, comandos FTP, comandos TFTP, descarga de comandos XModem, comandos de administración de usuarios, y los comandos de propiedades de nivel.

Cuando el equipamiento es nuevo, las contraseñas son las utilizadas por defecto por la tecnología utilizada y lo primero que se debe hacer es cambiarlas por motivos de seguridad y administración.

Es importante definir primeramente que usuarios van a tener acceso al equipo para asignarle un nivel y posteriormente la contraseña. Para que la seguridad funcione adecuadamente se deben crear políticas y lineamientos de seguridad a nivel internos y capacitar al personal para hacerlas cumplir.

CAPITULO 4. SIMULACIÓN DEL DISEÑO DE TOPOLOGÍA LÓGICA DE LA RED DE DATOS DE UN ENTE DEL MIDENA.

4.1 INTRODUCCIÓN

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.

Es importante tener en cuenta que la institución cuenta con equipamiento de tecnología 3Com, el mismo que presenta algunas funciones no aplicables a otras tecnologías del mercado, por lo cual este capítulo se dividirá en dos partes: la primera enmarcará todas las configuraciones realizadas en equipamiento 3Com; mientras que en la segunda parte se desarrollará la simulación para validar la funcionalidad del modelo propuesto con un simulador del mercado. Es importante mencionar que si bien cada tecnología presenta ciertas particularidades de configuración, la funcionalidad de los equipos (con características similares) es la misma.

4.2 TOPOLOGÍA

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.

4.2.1 TOPOLOGÍA FÍSICA

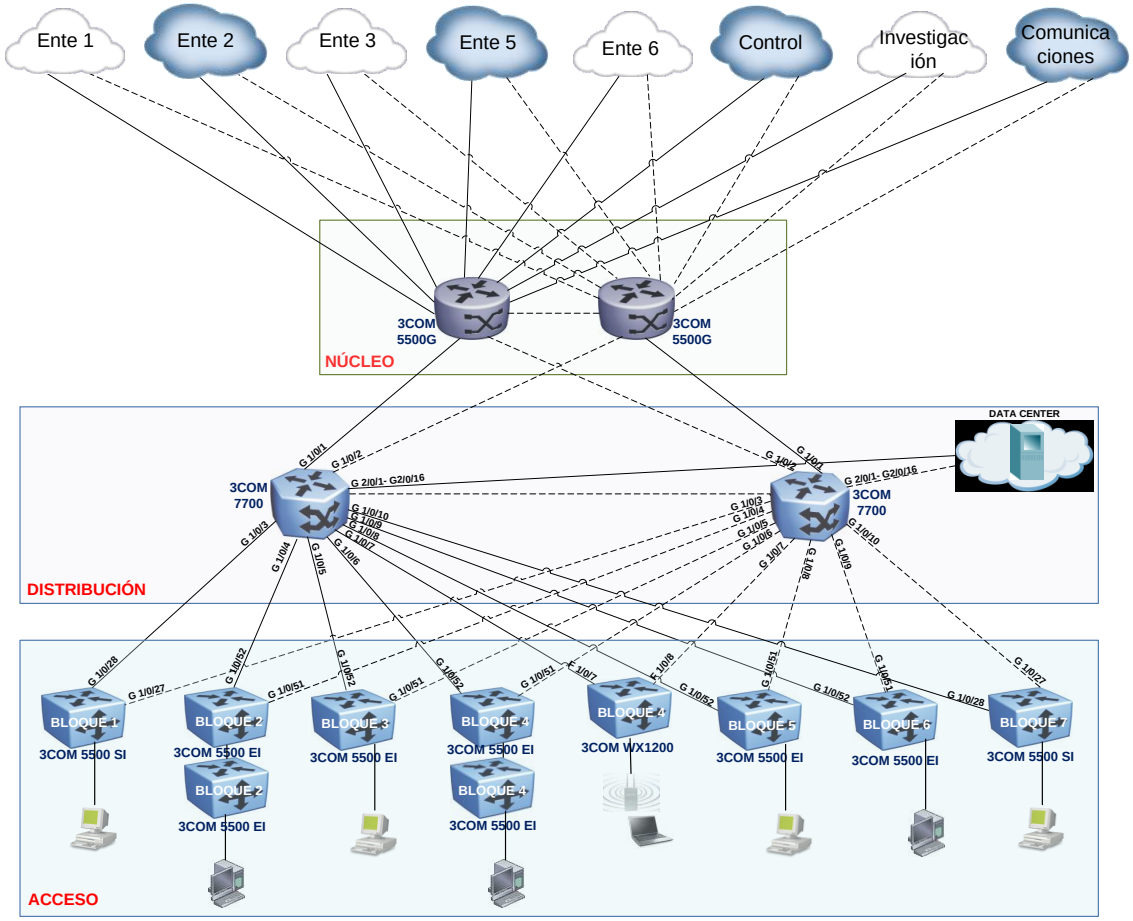


Figura 57. Topología física de la red

Fuente: Nancy Yolanda Ramón I.

4.2.2 TOPOLOGÍA LÓGICA

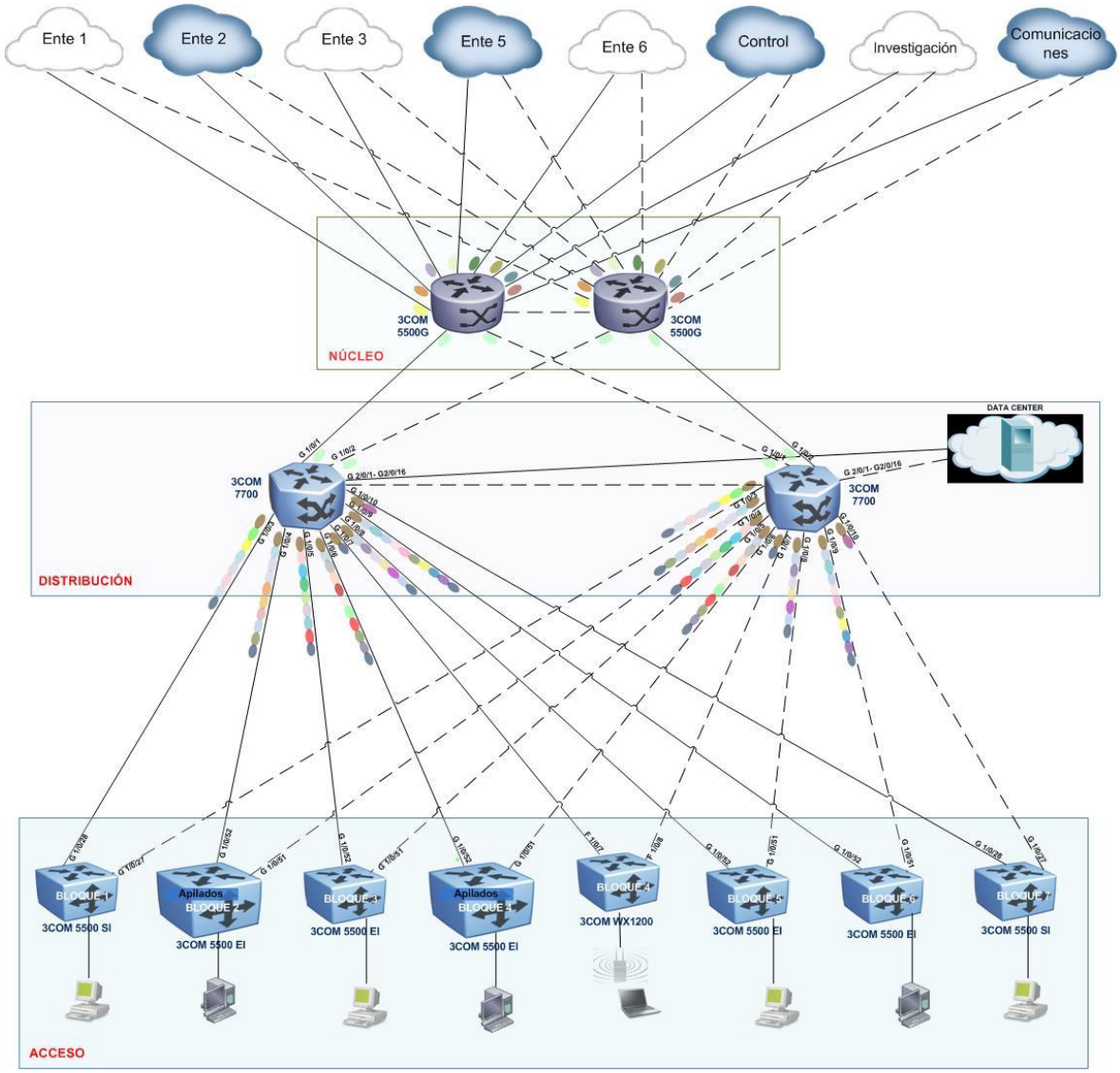


Figura 58. Topología lógica de la red

Fuente: Nancy Yolanda Ramón I.

La distribución de VLAN utilizada en la figura 58 se amplía en la siguiente figura:

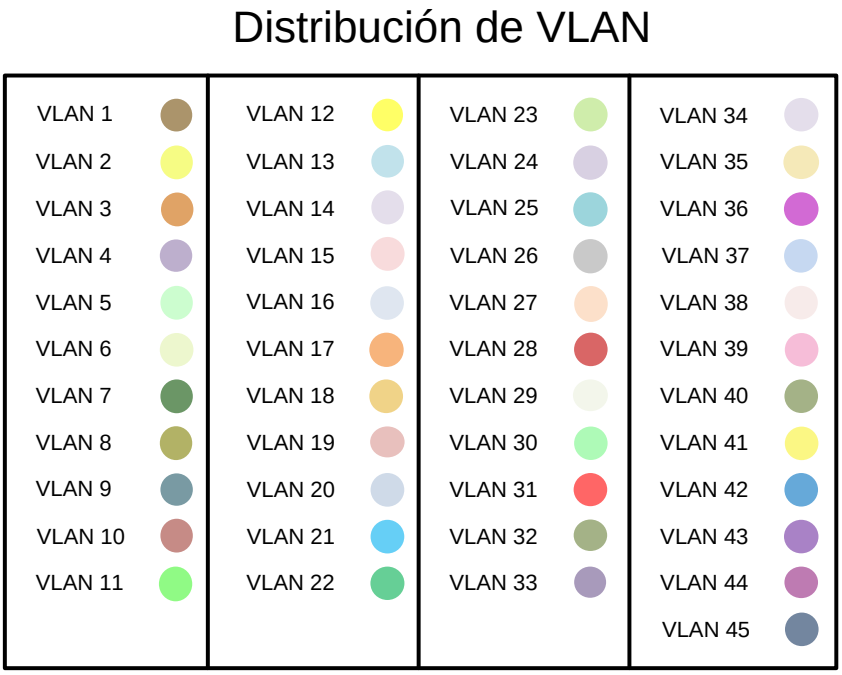


Figura 59. Distribución de VLAN

Fuente: Nancy Yolanda Ramón I.

4.3 CONFIGURACIONES

Como se observó en el levantamiento de la infraestructura de red realizada en el capítulo 2, la tecnología utilizada en la institución es 3Com, por lo tanto el desarrollo de la configuración será realizada en base a la misma. Los documentos de apoyo para la realización de las configuraciones fueron tomadas de los datasheet[90] del equipamiento existente.

Dentro de las configuraciones a realizarse en el equipamiento de red es importante que se tome en cuenta las configuraciones básicas que deben desarrollarse en todos los equipos, dado que constituyen las configuraciones mínimas a realizarse en cada uno de ellos de manera que se asegure tanto la facilidad de administración de manera remota utilizando protocolos seguros, como la implementación de seguridades en los mismos. Luego de realizadas dichas configuraciones deben realizarse las configuraciones necesarias para cada uno de los equipos en función de la capa a la cual den servicio.

[90] Tomados de la página oficial de h3c http://h17007.www1.hp.com/us/en/

4.3.1 CONFIGURACIONES BÁSICAS

Los equipos marca 3Com permiten su administración por medio de una interfaz de línea de comandos CLI[91]. Los comandos de administración se encuentran agrupados por medio de niveles, lo cual evita que usuarios no autorizados realicen cambios en los mismos al no tener los permisos suficientes para ello.

Los comandos están agrupados en base a cuatro niveles: Visit, Monitor, Manager y Administrator, dependiendo del grupo los comandos habilitados para la administración y gestión del equipamiento activo.

La administración presenta dos modos de vista de comandos que son:

- **<SW5500>** Vista de Usuario.
- **[SW5500]** Vista de Sistema.

La vista de usuario es mostrada al ingresar al equipo, los comandos permitidos en este modo se asocian a la información básica del switch; en cambio el modo de vista de sistema permite configurar el switch. Para pasar de la vista de usuario a la vista de sistema se debe introducir el comando *system-view*.

Independientemente de la capa de red en la cual se trabaje, es importante que se realicen ciertas configuraciones básicas que permitan administrar y gestionar el equipamiento de una manera segura, las configuraciones más importantes se muestran a continuación.

4.3.1.1 Configuración de usuarios

Dado que en función del nivel con el que se ingrese al equipamiento (Nivel 0 - 3) están dados los privilegios de configuración, es necesario que se proteja su acceso, determinándose como primer punto los usuarios con el respectivo nivel de acceso y las contraseñas a configurarse. Su configuración está basada en el siguiente procedimiento:

1 Definir el nombre del nuevo usuario.
2 Definir la contraseña para el nuevo usuario. Ésta puede ser:

[91] CLI: Command Line Interface (Interfaz de Línea de Comandos)

Simple: la contraseña se guarda en texto plano.

Cifrada: la contraseña se guarda en texto cifrado.

3 Definir el tipo de servicio de acceso.

4 Definir el nivel de acceso (0 – 3) que se le asignará al usuario.

A continuación se muestra una vista de la configuración desarrollada con tres diferentes usuarios y niveles de acceso.

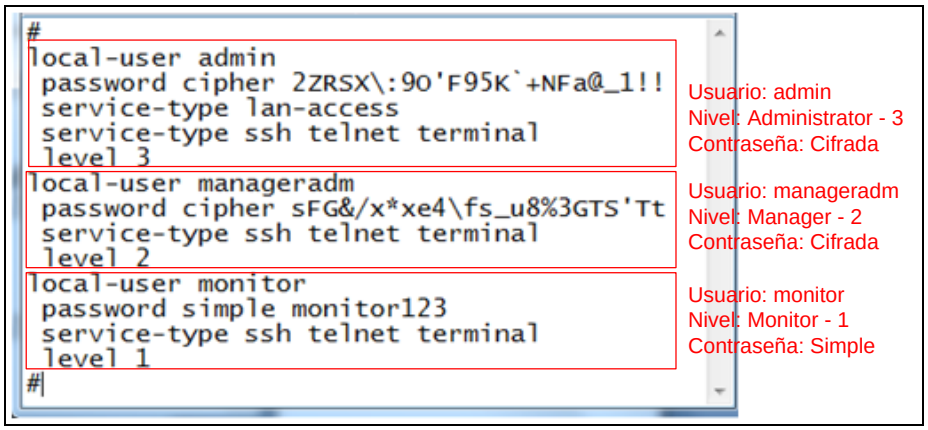


Figura 60. Vista de configuración de usuarios

Fuente: Consola de Administración Remota – 3Com

Es importante tener en cuenta que la contraseña debe estar cifrada para evitar que la misma pueda ser identificada, en especial en los niveles 2 y 3 los cuales pueden realizar cambios en la configuración. No se debe olvidar que por seguridad las contraseñas correspondientes a los diferentes niveles de accesos deben ser cambiadas.

4.3.1.2 Configuración de la dirección IP del equipo

Para permitir que el switch sea administrado de manera remota debe contar con una dirección IP dentro de la subred designada para el equipamiento activo. La configuración de la dirección IP se desarrolla mediante los siguientes pasos:

1 Ingresar a la interfaz de administración - Vlan 1.

2 Asignar la dirección IP utilizada para administración del equipo.

Luego de realizada la respectiva configuración es importante que se valide el acceso desde la subred de administración.

Con la configuración de la dirección IP de administración se puede contar con un acceso remoto tipo telnet, el cual se encuentra activado por defecto, sin embargo no es un protocolo de acceso seguro. La vista de la configuración realizada se muestra a continuación:

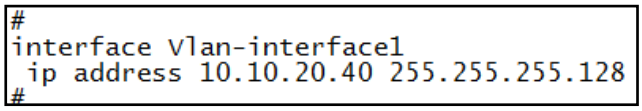


Figura 61. Vista configuración dirección IP de administración

Fuente: Consola de Administración Remota – 3Com

4.3.1.3 Configuración de acceso SSH[92]

Secure Shell es un protocolo que permite el ingreso a los servidores o equipos de red de manera remota para realizar configuraciones desde o hacia el equipo remoto de forma segura al emplear mecanismos de encripción que permiten proteger la información. A diferencia de telnet o rlogin, SSH encripta la sesión de registro impidiendo que alguien pueda obtener la contraseña.

Debido que SSH utiliza mecanismos para proteger tanto los datos para el establecimiento de la conexión como para el intercambio de datos es conveniente el uso de este protocolo de comunicación para la administración y gestión del equipamiento activo de forma remota.

Antes de configurar un acceso SSH se debe realizar previamente la configuración de un usuario con acceso SSH como se explicó en el apartado *4.3.1.1 Configuración de usuarios*, posterior a ello se realiza la siguiente configuración dentro de la interfaz vty:

1. Definir el esquema de autenticación.
2. Definir SSH como tipo de autenticación y protocolo de entrada.

La configuración para definir el acceso ssh se muestra en las figuras 62 y 63.

[92] SSH: *Secure Shell*

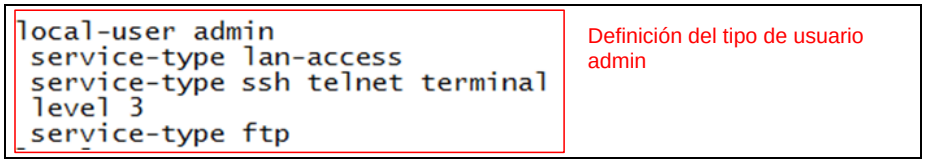


Figura 62. Vista configuración de usuarios

Fuente: Consola de Administración Remota – 3Com

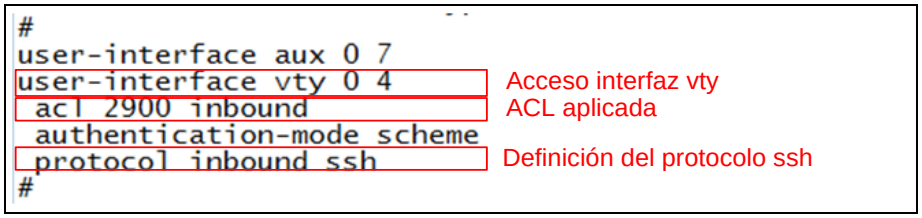


Figura 63. Vista configuración para acceso vty – ssh

Fuente: Consola de Administración Remota – 3Com

4.3.1.3.2 Acceso SSH desde una estación cliente

Una vez establecido como protocolo de entrada para la administración remota del equipamiento activo el protocolo SSH, es importante definir el cliente utilizado para el acceso desde la estación remota.

Un programa gratuito que permite realizar conexiones remotas utilizando el protocolo SSH es putty.

Al ejecutar el programa se ingresa a una interfaz de administración desde la cual se puede configurar accesos remotos hacia los diferentes equipos o servidores.

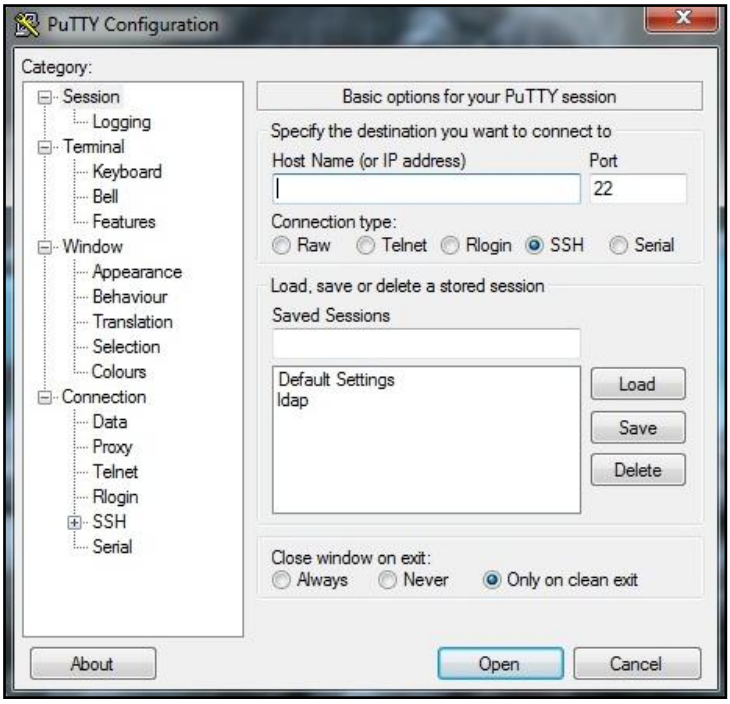


Figura 64. Vista configuración programa putty

Fuente: Software Putty

Para ingresar a un equipo basta con especificar la dirección IP, seleccionar protocolo SSH y hacer clic sobre Open.

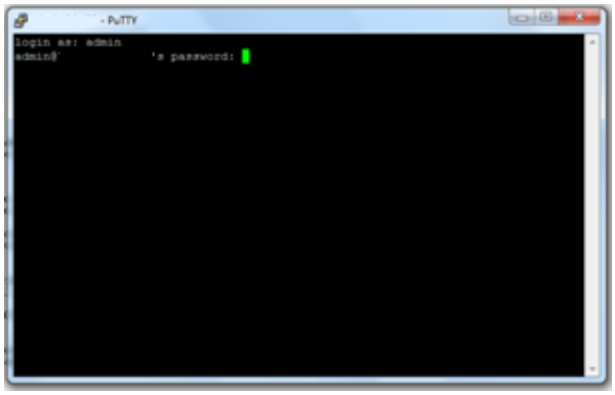


Figura 65. Vista de ventana de acceso remoto

Fuente: Consola de Administración Remota - Putty

Una vez abierta la conexión se pedirá el usuario y contraseña para acceso remoto declarada en el equipo, si la conexión es exitosa ingresará a la administración mediante línea de comandos, caso contrario se volverá a pedir usuario y contraseña de validación correctos.

4.3.1.4 Configuración de banners

El objetivo de configurar un banner es presentar un mensaje de información, bienvenida o advertencia a las personas que ingresen al equipo. Para configurar un banner se debe ingresar el comando *header login* seguido del texto a mostrar de la siguiente manera:

```
#
 header login %<< SW-BLOQUE2 -- ACCESO
RESTRINGIDO >>%
#
```

Figura 66. Vista configuración de Banner

Fuente: Consola de Administración Remota – 3Com

Luego de haber configurado el banner cuando se produzca un acceso se mostrará el mensaje de la siguiente manera:

```
**********************************************************
*           All rights reserved (1997-2005)              *
*      Without the owner's prior written consent,        *
*no decompiling or reverse-engineering shall be allowed.*
**********************************************************

<< SW-BLOQUE2 -- ACCESO RESTRINGIDO >>

Login authentication


Username:admin
Password:
% Login failed!

Username:admin
Password:
```

Figura 67. Vista de banner de acceso configurado

Fuente: Nancy Yolanda Ramón I.

4.3.1.5 Actualización de la versión de SO[93]

Las actualizaciones de versión de SO son aplicables cuando se desea agregar nuevas funcionalidades a los equipos o cuando la finalidad es aplicar parches de seguridad incluidas en las nuevas versiones.

Para actualizar el SO se debe seguir el siguiente procedimiento:

1. Copiar a flash la nueva versión de Sistema Operativo

[93] SO: Sistema Operativo

2. Especificar el Sistema Operativo para el siguiente buteo
3. Guardar la configuración realizada
4. Reiniciar el equipo

Para validar la configuración realizada se debe verificar la versión del SO.

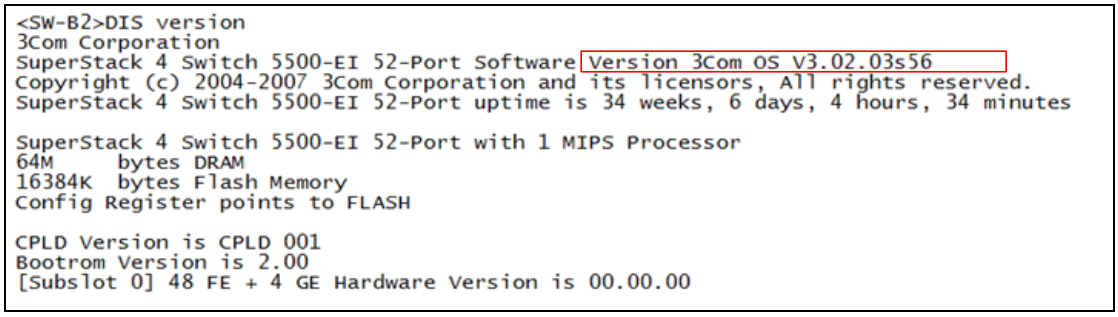


Figura 68. Vista de la versión de SO

Fuente: Consola de Administración Remota – 3Com

4.3.1.6 Habilitación de SNMP

SNMP permite obtener estadísticas sobre el uso de los recursos y con la ayuda de algún tipo de software que se comunique con el equipamiento como Nagios, HP OpenView, MRTG, OpenNMS, entre otros, y obtener los valores recogidos para generar mencionadas estadísticas.

Para activar SNMP es importante asignar las comunidades de lectura del equipamiento. El procedimiento para activarlos es el siguiente:

1. Asignar la comunidad de lectura.
2. Habilitar la versión de SNMP.

Así también de forma opcional se puede ingresar información referente al contacto y ubicación. La configuración se muestra de la siguiente manera:

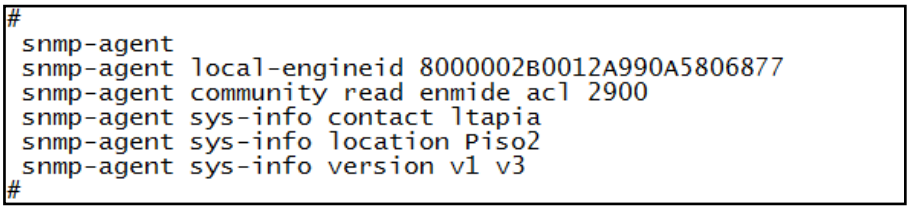


Figura 69. Vista de configuración de SNMP

Fuente: Consola de Administración Remota – 3Com

4.3.2 CONFIGURACIONES BASADAS EN CAPAS

Una vez realizadas las configuraciones básicas en cada uno de los equipos que integran el modelo es importante definir las configuraciones relacionadas a la capa en dependencia de la funcionalidad de cada una de ellas.

4.3.2.1 Capa de núcleo

Dado que ésta capa constituye el backbone de las comunicaciones de la Red de Datos es importante determinar las configuraciones que permitan brindar la conectividad con los diferentes Entes del Ministerio, teniendo en cuenta la seguridad que debe brindarse, además de asegurar su disponibilidad, permitir la configuración de un protocolo de enrutamiento dinámico, entre otros. A continuación se detallan las configuraciones realizadas a nivel de esta capa resaltando sus componentes principales de configuración, los ejemplos de configuraciones serán tomadas del equipo 3Com 5500G ubicado en Centro de Conmutación.

4.3.2.1.1 Configuración de VLAN

Como se muestra en la configuración de la figura 55, las vlan a nivel de la capa de núcleo permiten brindar seguridad hacia los diferentes Entes del Ministerio de Defensa así también mejorar la calidad del servicio al segmentar el tráfico y los dominios de broadcast generados en él.

Por defecto, la única vlan configurada en el equipamiento activo es la vlan 1 desde la cual se permite gestionar el equipo y a la cual pertenecen todos los puertos.

A éste nivel es importante crear y asignar las vlan necesarias para brindar el servicio requerido, tomando como base la Tabla 20. *Direccionamiento IP para enlaces de la red de datos*, creándose una vlan por cada red manejada desde el Centro de Conmutación, el procedimiento a seguir es el siguiente:

1. Crear las vlan en base al id indicado.
2. Definir el nombre para la vlan creada.
3. Ingresar la descripción de la vlan definida.

A pesar de que los pasos 2 y 3 son opcionales dentro de la configuración, son necesarios para una mejor gestión y administración del equipamiento ya que permite tener una visión clara de la configuración realizada.

Una vez creadas las vlan según el diseño previamente detallado es necesario que se asigne el correspondiente direccionamiento IP de cada una de ellas basándose en la tabla 20.

La declaración de las vlans creadas debe realizarse de la siguiente manera:

1. Ingresar a la interfaz de la vlan.
2. Asignar el direccionamiento IP de la vlan.

Adicionalmente se puede agregar una descripción a la interfaz de la vlan, para facilitar tareas de administración y gestión de la red. La configuración realizada se muestra a continuación:

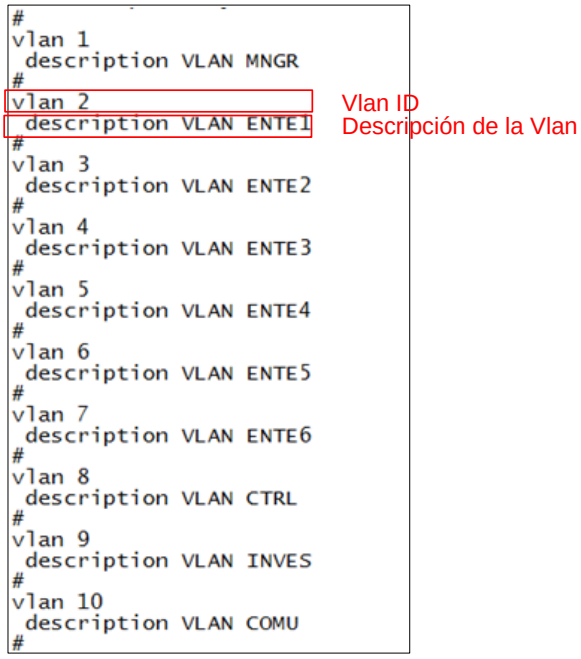


Figura 70. Vista creación de vlan – Capa Núcleo

Fuente: Consola de Administración Remota – 3Com

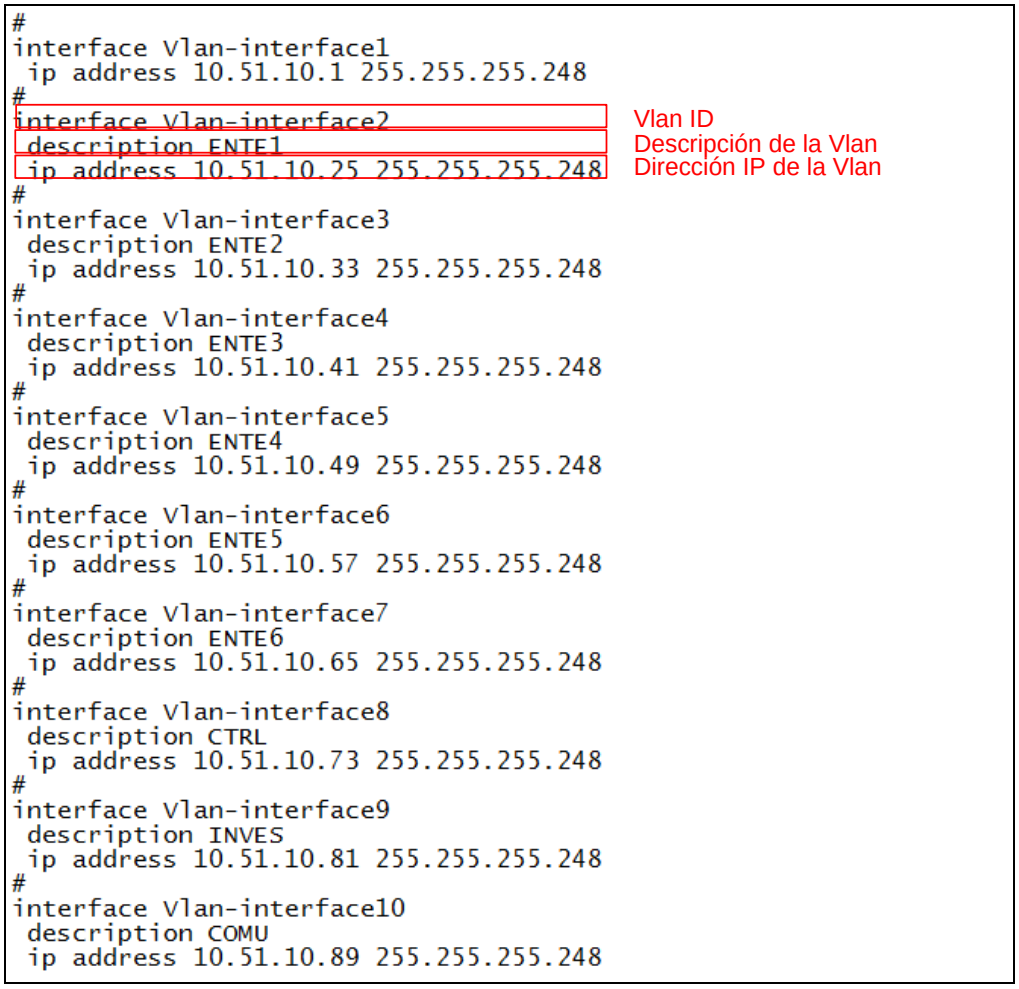


Figura 71. Vista declaración de vlan – Capa Núcleo

Fuente: Consola de Administración Remota – 3Com

4.3.2.1.2 Configuración de puertos de acceso

Una vez declaradas las vlan correspondientes a éste nivel se deben configurar los puertos de conexión hacia cada uno de los respectivos entes en base a la distribución realizada en la tabla 20. Para ello es necesario realizar los siguientes pasos.

1. Ingresar al puerto de conexión utilizado para la conexión.
2. Declarar al puerto como tipo de acceso.
3. Agregar la Vlan al puerto.

La configuración realizada se muestra a continuación.

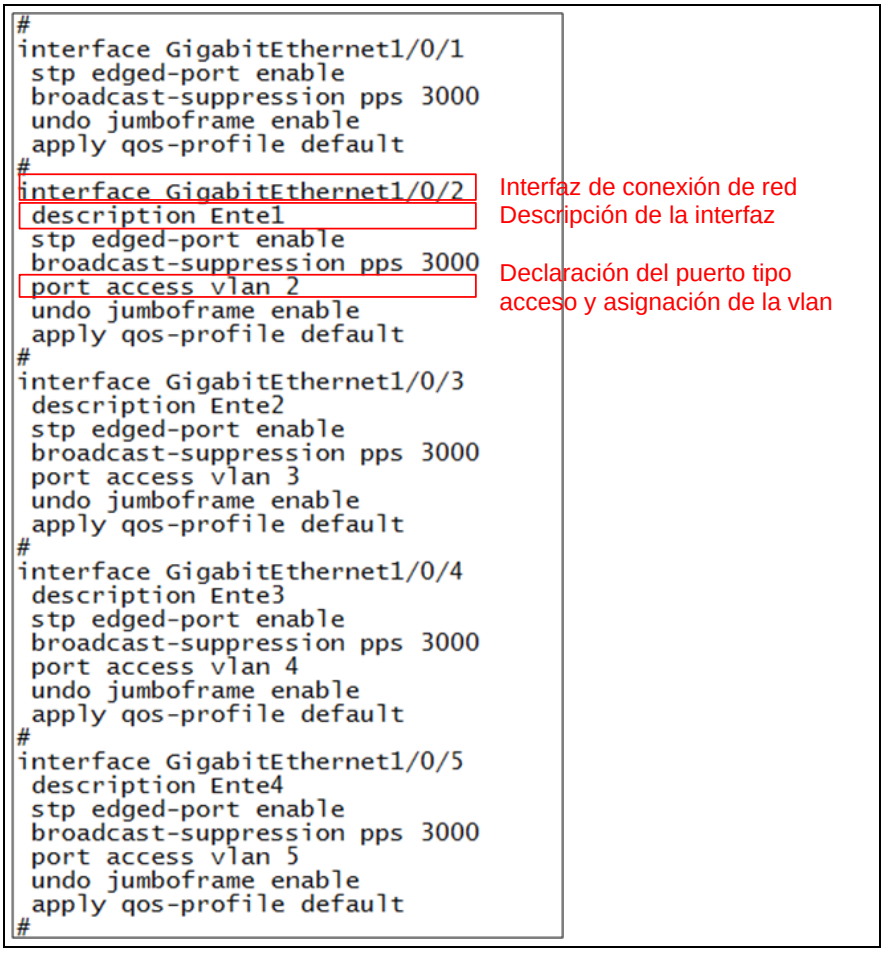


Figura 72. Vista configuración puertos de acceso

Fuente: Consola de Administración Remota – 3Com

4.3.2.1.2 Configuración de puertos trunk

En caso de ser necesario trabajar con más de una vlan por los puertos de conexión hacia las respectivas fuerzas se debe utilizar puertos tipo trunk. El procedimiento a realizarse es el siguiente:

1. Ingresar al puerto utilizado para la conexión
2. Declarar al puerto como tipo trunk
3. Permitir el paso de las vlan´s requeridas

En el caso de la actual configuración no es necesario la aplicación de este tipo de puertos debido a que hacia cada uno de los Entes manejará una vlan determinada, asignada de forma específica a cada Ente.

4.3.2.2.4 Habilitación de Alta Disponibilidad

El manejar el backbone principal de comunicaciones al interior del Ministerio de Defensa es importante que su infraestructura tenga en cuenta características de alta disponibilidad para asegurar su conectividad, para ello se debe habilitar el protocolo MSTP, siguiendo el siguiente procedimiento:

1. Habilitar el protocolo stp
2. Configurar la región stp
3. Activar las características de la región mstp
4. Establecer el equipo root en base a las instancias establecidas
5. Habilitar el protocolo stp en los puertos determinados

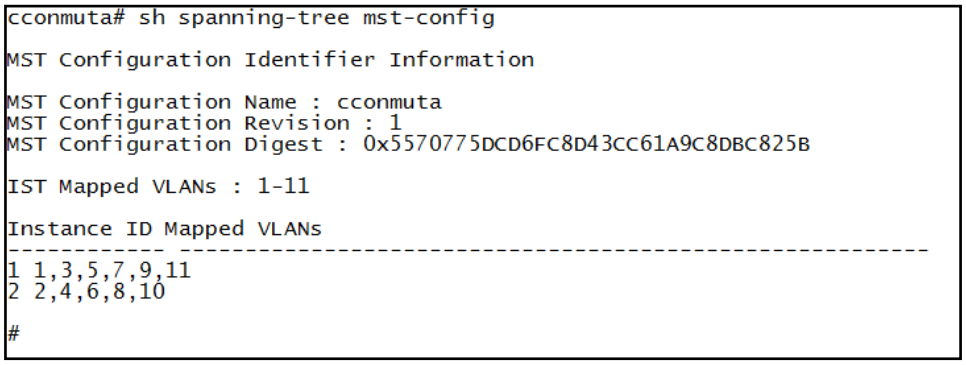


Figura 73. Vista de configuración MSTP

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.5 Habilitación de protocolos de enrutamiento dinámico

Tomando en cuenta el protocolo de enrutamiento utilizado de manera estándar en la institución (OSPF), además de las características de la red, es necesario realizar la configuración del protocolo de enrutamiento dinámico OSPF. La configuración estará basada en:

1. Definir el protocolo de enrutamiento
2. Definir el id de área
3. Configurar las redes conectadas directamente

Luego de realizar el procedimiento indicado es necesario que se valide las tablas de enrutamiento, verificando las redes a las cuales se debe tener acceso de manera que se asegure la conexión hacia los diferentes entes del mismo.

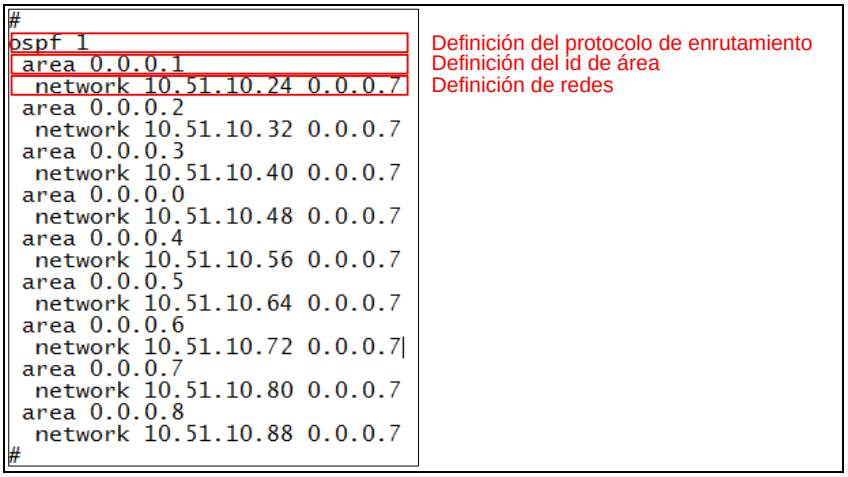


Figura 74. Vista protocolo de enrutamiento dinámico

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.6 Configuración de Control de Acceso

Teniendo en cuenta que uno de los principales objetivos del modelo propuesto es la seguridad, es importante que se defina el tráfico que se permitirá cursar en la red, para ello es importante tener en cuenta el proceso indicado:

1. Definir el tráfico permitido a cursar en la red
2. Definir el tráfico no permitido a cursar en la red
3. Aplicar las acl indicadas en los puertos de conexión

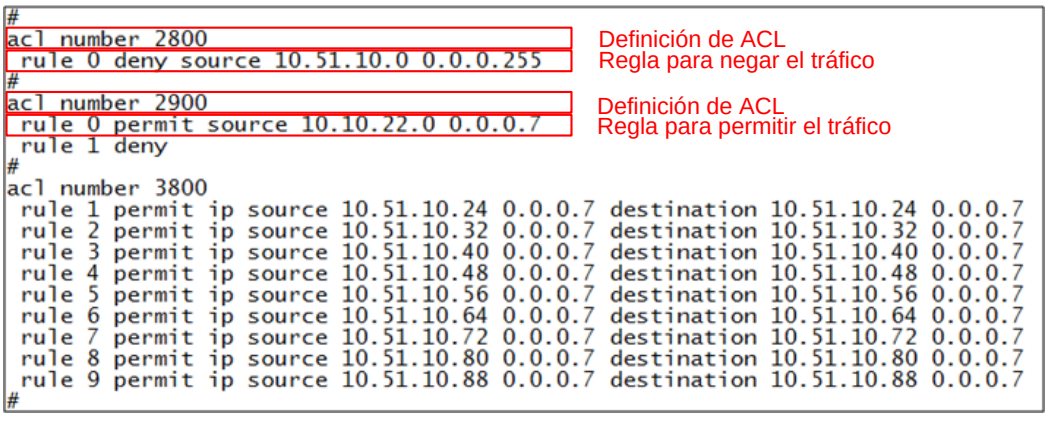


Figura 75. Definición de ACL para el control de tráfico

Fuente: Consola de Administración Remota – 3Com

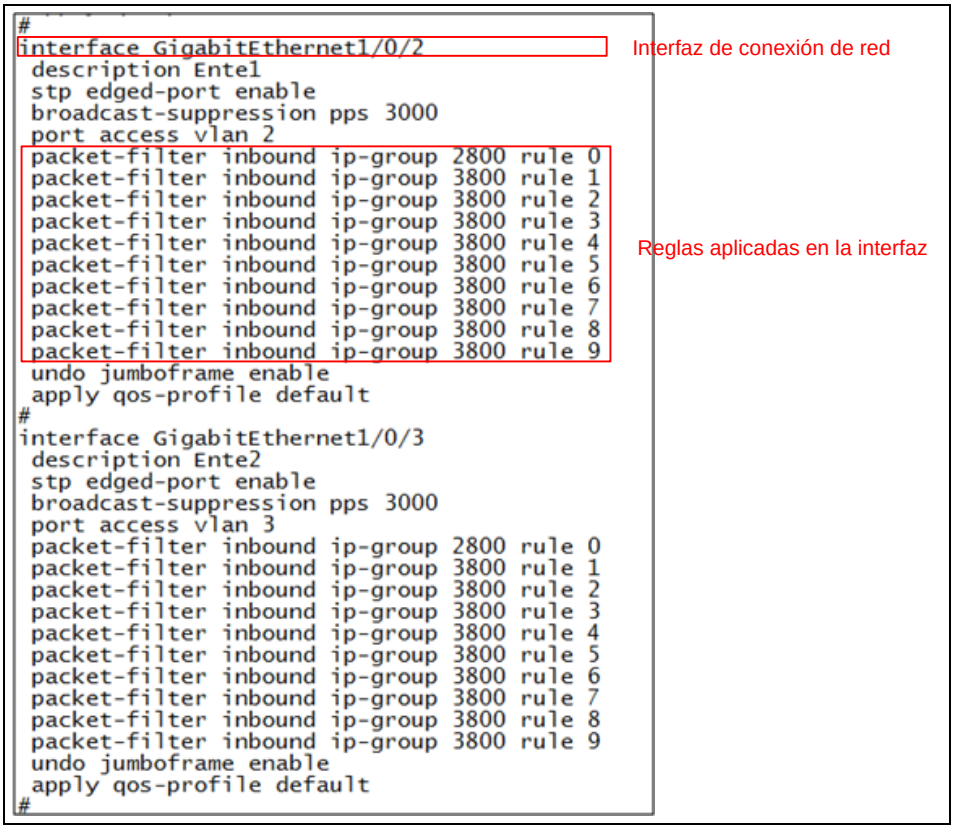


Figura 76. Definición de filtrado de tráfico en puertos de conexión

Fuente: Consola de Administración Remota – 3Com

Adicional al control de tráfico generado en la red, es importante definir mediante listas de control de acceso los usuarios permitidos para ingresar a la administración del equipamiento mediante el terminal virtual. El procedimiento para realizar la configuración es el siguiente:

1. Definir la vlan con acceso para la administración del equipamiento
2. Aplicar las ACLs creadas dentro de la interfaz vty

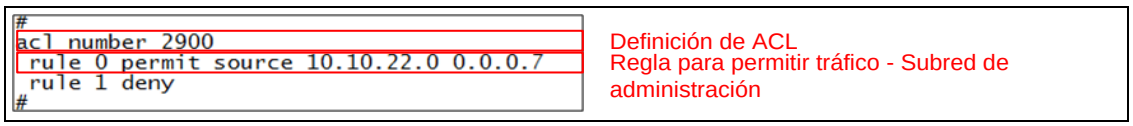


Figura 77. Vista ACL determinada para administración del equipo

Fuente: Consola de Administración Remota – 3Com

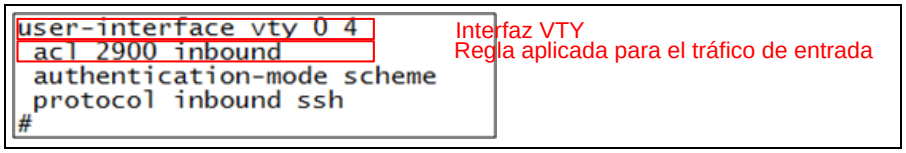


Figura 78. Vista ACL de administración mediante interfaz vty

Fuente: Consola de Administración Remota – 3Com

5.3.2.2 Capa de distribución

En la capa de distribución se manejará tráfico generado tanto hacia el nivel de núcleo como hacia el nivel de acceso. Por un lado hacia el nivel de núcleo se manejará el tráfico enviado y recibido de la red de datos, en cambio en el caso de la capa de acceso se manejará todo el tráfico generado internamente por la institución, por lo cual en esta capa entre sus principales configuraciones es necesario manejar disponibilidad de servicio, seguridad, enrutamiento, entre otros.

Las configuraciones tomadas como ejemplo en el desarrollo, serán tomadas del equipo 3Com 7750.

4.3.2.2.1 Configuración de VLAN

A este nivel es necesario configurar las vlan que serán utilizadas para la segmentación de tráfico y dominios de broadcast de la red tanto del nivel de núcleo como para acceso. La declaración de las vlan estará dada en función de la tabla 21.

Para realizar su configuración se debe seguir el siguiente procedimiento:

1. Declarar la vlan determinada en función del ID.
2. Agregar una descripción para la vlan
3. Agregar un nombre que identifique a la vlan

Los numerales 2 y 3 no son obligatorios sin embargo facilitan la administración del equipamiento.

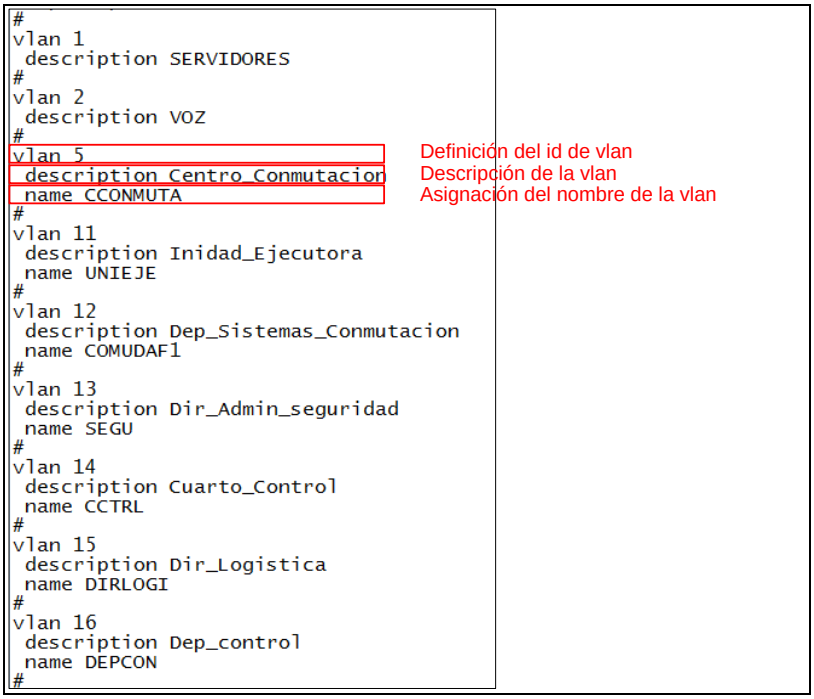


Figura 79. Vista creación de vlan - Capa Distribución

Fuente: Consola de Administración Remota – 3Com

Además teniendo en cuenta que los equipos de esta capa serán los encargados de manejar el enrutamiento inter-vlan es importante que se asigne el correspondiente direccionamiento IP de las vlan utilizadas a nivel de acceso.

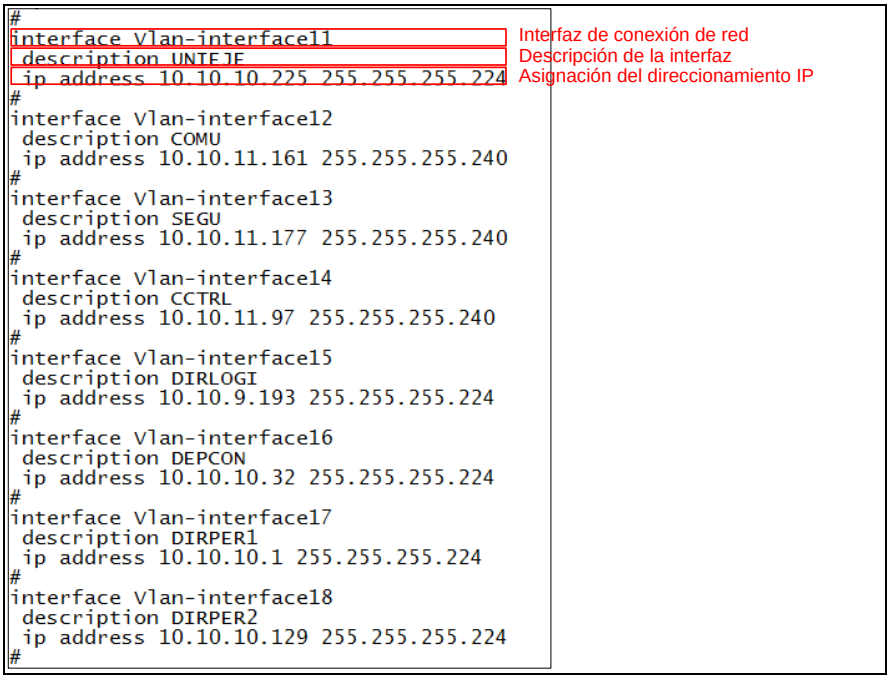


Figura 80. Vista declaración de vlan - Capa Distribución

Fuente: Consola de Administración Remota – 3Com

En esta capa se manejarán dos tipos de puertos, tipo acceso y tipo trunk, en función del nivel al cual se brindará la conexión.

4.3.2.2.2 Configuración de puertos de acceso

Hacia la capa de núcleo solo se manejará una vlan por lo cual se configurará puertos de tipo acceso para asegurar la conexión y seguridad hacia esta capa. Así también para la conexión de los servidores de aplicación se utilizará este tipo de puertos; para su configuración el procedimiento es el siguiente:

1. Crear la vlan, en base al id de la tabla 21
2. Definir los puertos miembros de la vlan

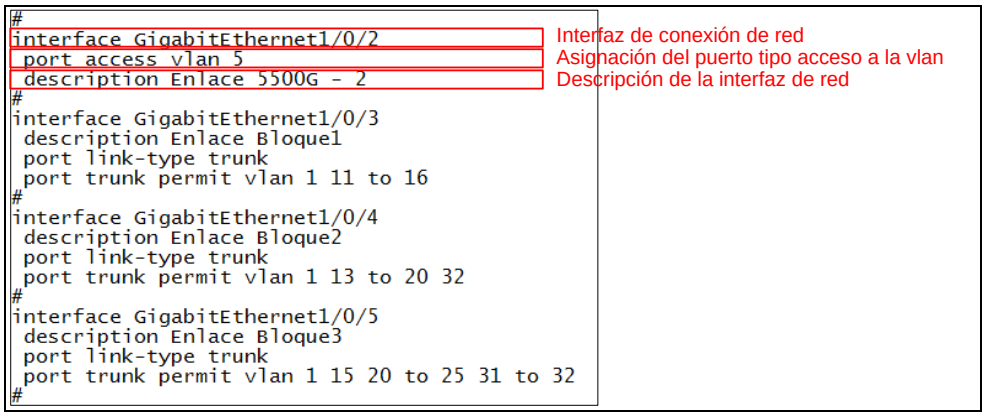


Figura 81. Vista configuración de puertos acceso - Capa distribución

Fuente: Consola de Administración Remota – 3Com

Es importante que se agregue una descripción al puerto, la cual facilite la gestión y administración del equipamiento de red.

4.3.2.2.3 Configuración de puertos trunk

Para la comunicación hacia la capa de acceso se deberá permitir el paso de múltiples vlans en el puerto de conexión por lo cual se asignarán puertos configurados en tipo trunk. El procedimiento utilizado para realizar la configuración es la siguiente:

1. Crear vlan, según la tabla 21
2. Configurar la interfaz de la vlan con la dirección IP
3. Configurar el puerto de conexión tipo trunk

4. Asignar las vlan permitidas para pasar por el puerto trunk

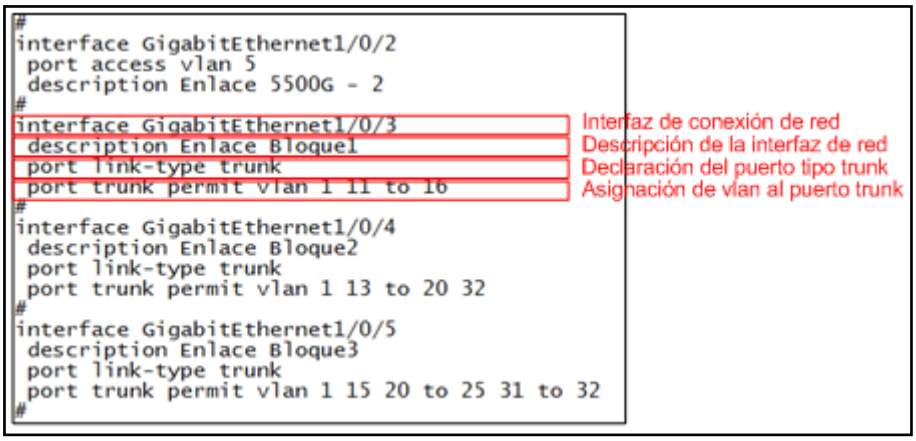


Figura 82. Vista configuración puertos tipo trunk - Capa Distribución

Fuente: Consola de Administración Remota – 3Com.

Así también en los puertos de conexión es recomendable que se asigne una descripción lo cual facilite la identificación y administración de los puertos asignados.

4.3.2.2.4 Habilitación de Alta Disponibilidad

Al manejar esta capa todo el tráfico tanto hacia la capa de núcleo como hacia la capa de acceso es importante que se brinde alta disponibilidad, asegurando la conexión debido a que esta capa conforma un punto crítico en la red interna, por tanto se debe tener un cuidado especial debido a que de ocurrir algún daño se perdería incluso la comunicación a nivel interno.

Para realizar su configuración se debe realizar el siguiente procedimiento:

1. Habilitar el protocolo stp
2. Configurar la región stp
3. Activar las características de la región MSTP, dado que se manejarán múltiples vlan por un mismo enlace.
4. Establecer el equipo root en base a las instancias establecidas
5. Habilitar el protocolo stp en los puertos determinados

4.3.2.2.5 Habilitación de protocolos de enrutamiento dinámico

Teniendo en cuenta el protocolo de enrutamiento utilizado como estándar a nivel de la red es necesario que se habilite el enrutamiento OSPF de manera que se tenga comunicación a nivel de la red de datos. Para esto es importante tener en cuenta el área asignada hacia la institución y realizar el procedimiento que se detalla a continuación:

1. Definir el protocolo de enrutamiento
2. Definir el id de área
3. Configurar las redes conectadas directamente

Luego de realizar el procedimiento indicado es necesario que se valide las tablas de enrutamiento, verificando las redes a las cuales se debe tener acceso de manera que se asegure la conexión hacia los diferentes entes del mismo.

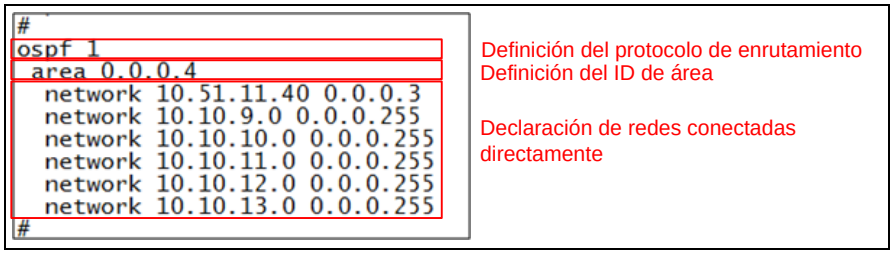


Figura 83. Vista del protocolo de enrutamiento dinámico - Capa Distribución

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.6 Configuración de Control de Acceso

Es importante tener control sobre la administración del equipamiento de red, asegurando el ingreso mediante una conexión remota de únicamente el personal autorizado desde una red determinada. Para realizar esta configuración se debe seguir el siguiente procedimiento:

1. Definir la vlan con acceso para la administración del equipamiento
2. Aplicar las ACLs creadas dentro de la interfaz vty

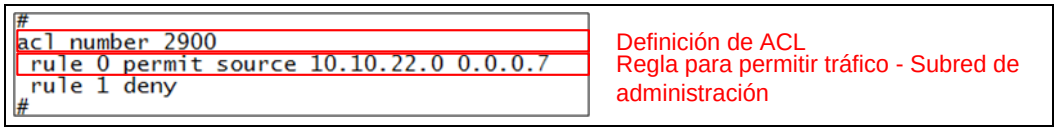


Figura 84. Vista de ACL 2900 - Capa distribución

Fuente: Consola de Administración Remota – 3Com

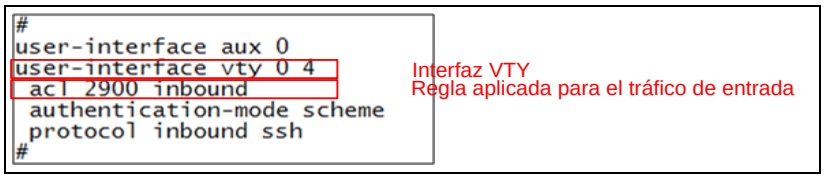


Figura 85. Vista configuración interfaz vty - Capa Distribución

Fuente: Consola de Administración Remota – 3Com

4.3.2.3 Capa de acceso

Como principal objetivo de esta capa es brindar la conexión hacia el usuario final. Así también a este nivel se debe tener en cuenta aplicar seguridad a nivel de puerto lo cual constituya el primer filtro de seguridad hacia la red. Teniendo en cuenta que la mayor parte de tráfico será generada en este nivel es necesario que se apliquen reglas para el control de tráfico lo cual brinde seguridad y permita mejorar el rendimiento de la red al reducir los dominios de broadcast que se generen en la misma.

Los ejemplos de configuración están tomadas del equipo de conmutación 3Com 5500G del Bloque 1.

4.3.2.2.1 Configuración de VLAN

A este nivel es necesario que se configuren las vlan utilizadas para segmentar el tráfico y brindar seguridad a nivel de usuario final de red. La configuración de cada vlan está dada en función de la tabla 21, debiendo configurarse en cada uno de los equipos de conmutación las vlans determinadas en la etapa de diseño.

Su configuración se la realiza mediante el procedimiento detallado a continuación:

1. Declarar la vlan, determinada en función del ID.
2. Agregar una descripción para la vlan
3. Agregar un nombre que identifique a la vlan

Los puntos 2 y 3 no son obligatorios sin embargo facilitan la administración del equipamiento. A continuación se muestra un ejemplo de configuración de vlan en el equipamiento del Bloque1.

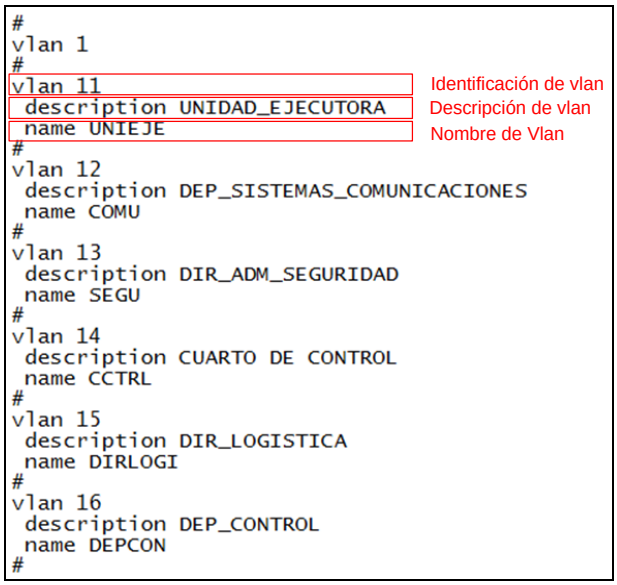


Figura 86. Vista de configuración de vlan – Capa de Acceso

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.2 Configuración de puertos de acceso

Luego de haber declarado las vlan necesarias en función del diseño a nivel de acceso se debe configurar los puertos asignados hacia nivel de usuario final basándose en el Anexo 4 "*Direccionamiento IP basado en VLAN*". Adicional a esta configuración es importante que se realice la configuración a nivel de estaciones de trabajo de manera que se habilite el acceso del usuario a la red, la configuración a realizarse en la tarjeta de red está dada en el Anexo 4.

La asignación de los puertos a una vlan puede realizarse de dos maneras como se indica a continuación:

Dentro de la vlan indicada.

1. Definir la vlan - determinada por el ID
2. Definir el puerto de conexión

Dentro de la interfaz deseada.

1. Definir el puerto de conexión
2. Definir el tipo de conexión del puerto
3. Declarar la vlan correspondiente

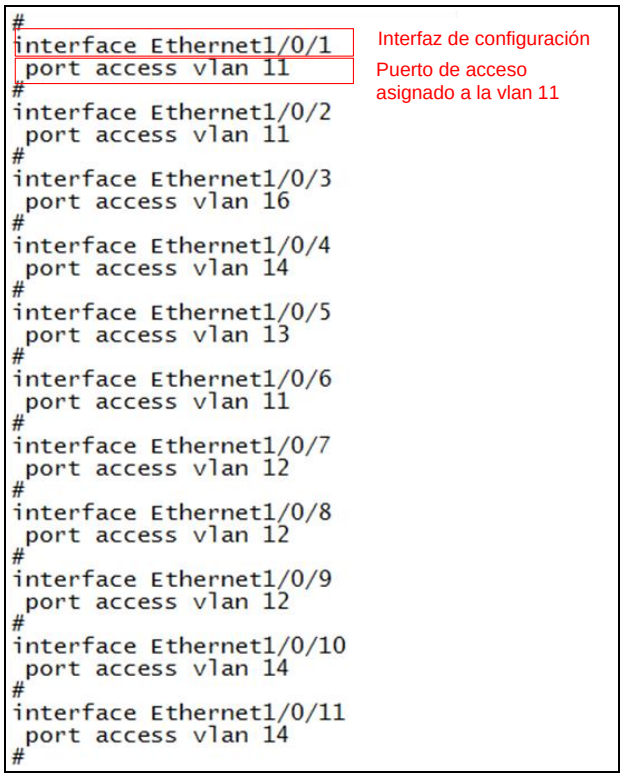


Figura 87. Vista configuración puertos tipo Acceso - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.3 Configuración de puertos trunk

Dado que cada uno de los bloques maneja diferentes vlan, es importante que se configuren puertos de conexión tipo trunk, debiendo identificarse los puertos utilizados como conexión hacia el equipamiento de distribución y las vlan que cursarán por ellos.

Para configurar los puertos trunk es necesario seguir el siguiente procedimiento.

1. Ingresar a la interfaz a configurarse
2. Definir el tipo de conexión del puerto
3. Declarar las vlans permitidas a cursar por la interfaz

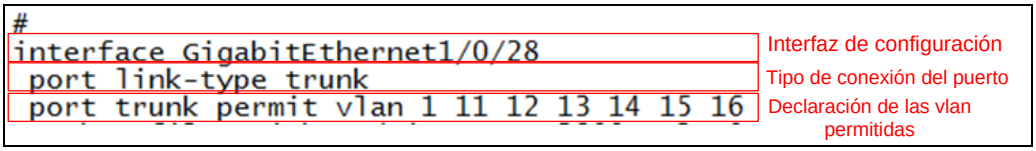


Figura 88. Vista configuración puertos tipo trunk - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.4 Configuración de Control de Acceso

Control de acceso a la red

En función de las consideraciones de diseño descritas en el capítulo anterior con el objetivo de prevenir el cambio de direcciones IP en los equipos de cómputo sin previa autorización, además, precautelar la seguridad de la institución al evitar que equipos fuera del parque informático de la institución se conecten a la red, se ha considerado la implementación del control de acceso a la red basada en la dirección MAC y dirección IP, obligando al puerto a trabajar con las especificaciones indicadas. Una vez que se ha realizado el enlace al puerto, el equipo solo envía paquetes de datos cuando la correspondencia sea idéntica, debiendo cumplirse los dos parámetros: dirección MAC e IP, de esta manera no solo se mejora la seguridad de la red sino que se mejora su control, administración y gestión.

Para realizar la configuración del control de acceso a la red basado en MAC e IP se debe seguir el siguiente procedimiento:

1. Ingresar a la interfaz de configuración
2. Asignar el control de acceso a la red basado en la dirección MAC y la dirección IP del usuario

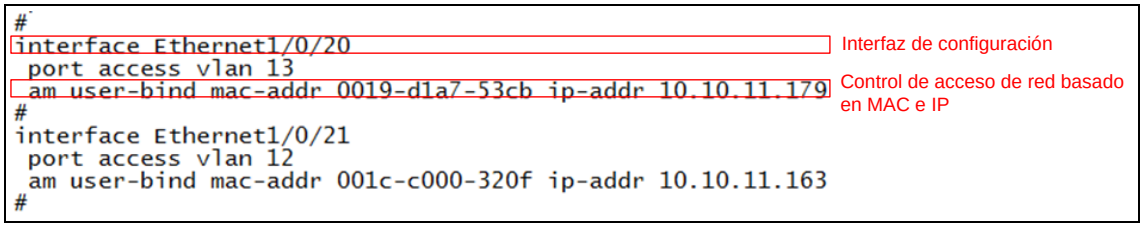


Figura 89. Vista configuración control de acceso a la red – Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Listas de Control de Acceso

Con el fin de limitar el tráfico intervlan es necesario que se configuren listas de control de acceso a nivel de los puertos de conexión con el equipo de distribución, así también es importante que se controle y limite la administración del equipamiento a la vlan de administradores. Para ello es necesario que se configuren tres diferentes tipos de listas de control de acceso como se indica a continuación:

Lista de control de acceso 2800

Con la configuración de la ACL 2800 se negará el tráfico entre las redes internas del edificio y se permitirá el tráfico de la subred perteneciente a la vlan de administradores de red. Su configuración está dada en función de:

1. Definir el número para la acl básica
2. Definir las reglas necesarias

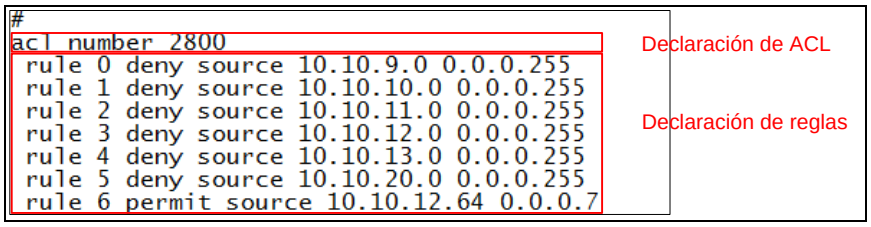


Figura 90. Vista configuración ACL 2800 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Con las reglas declaradas en la lista de acceso 2800 en primera instancia se encuentra negado todo el tráfico proveniente de las redes asignadas. De no crear alguna regla para permitir el tráfico en alguna de las subredes, las máquinas de los usuarios no tendrían conexión con ninguna de las demás subredes, ni con los miembros de la misma subred.

Sin embargo con las líneas anteriormente creadas simplemente se han creado las reglas pero aún no han sido aplicadas, para esto es necesario aplicar los filtros dentro de los puertos trunk.

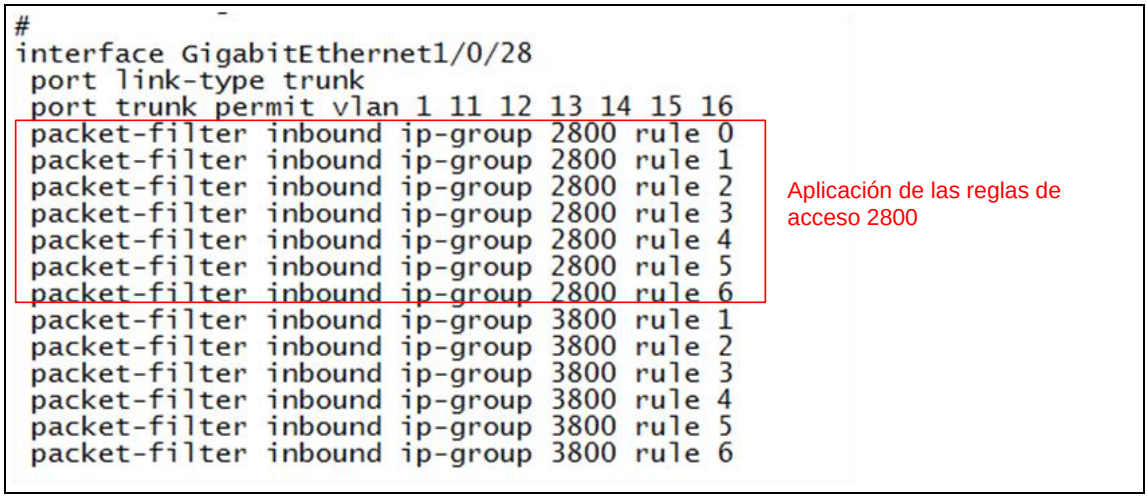


Figura 91. Vista aplicación reglas ACL 2800 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Lista de acceso 3800

La función de la lista de acceso 3800 es permitir que se genere tráfico entre los miembros de una vlan.

De igual forma que la lista de acceso 2800, las reglas pertenecientes a la lista de acceso 3800 se las configura en los puertos trunk de cada uno de switch de acceso.

A diferencia de las reglas de acceso 2800, estas deben ser configuradas dependiendo de su necesidad, es decir simplemente las subredes que estén configuradas en el switch, su asignación está dada en función de la regla asociada a cada una de las VLAN como se observa a continuación en la tabla 23:

Tabla 23. Asignación de ACL en función de la VLAN

VLAN	DEPENDENCIA	NOMBRE	NÚMERO ACL	LOCALIZACIÓN BLOQUES
Vlan 1	Servidores y Equipos	SRVEQU		DATACENTER
Vlan 3	Centro de Conmutación	CCONMUTA		DATACENTER
Vlan 11	Unidad Ejecutora	UNIEJE	Rule 1	B1
Vlan 12	Departamento de Sistemas/Comunic	COMU	Rule 2	B1
Vlan 13	Dirección Administrativa/Seguridad	SEGU	Rule 3	B1 - B2
Vlan 14	Cuarto de Control	CCTRL	Rule 4	B1 - B2

Vlan 15	Dirección de Logística	DIRLOGI	Rule 5	B1 - B3
Vlan 16	Departamento de Control	DEPCON	Rule 6	B1 - B2
Vlan 17	Dirección de Personal	DIRPER1	Rule 7	B2
Vlan 18	Dirección de Personal	DIRPER2	Rule 8	B2
Vlan 19	Asuntos Internacionales	ASUINT	Rule 9	B2
Vlan 20	Salas de Reuniones	SREU	Rule 10	B2 - B4 -B5 - B6
Vlan 21	Cuartel General	CGRAL	Rule 11	B3
Vlan 22	Departamento de Ingeniería	DEPING	Rule 12	B3
Vlan 23	Departamento de Contratación Pública	CONPUB	Rule 13	B3
Vlan 24	Dirección de Sanidad	SANIDAD	Rule 14	B3
Vlan 25	Departamento de Evaluación y Control	EVACTRL	Rule 15	B3 - B6
Vlan 26	Dirección de Telecomunicaciones	DIRTEL	Rule 16	B4
Vlan 27	Dirección de Sistemas	DIRSIST1	Rule 17	B4
Vlan 28	Dirección de Sistemas	DIRSIST2	Rule 18	B4
Vlan 29	Dirección de Sistemas	DIRSIST3	Rule 19	B4
Vlan 30	Dirección de Sistemas	ADMIN		B4
Vlan 31	Dirección Administrativa	DIRADM1	Rule 20	B3 - B4
Vlan 32	Dirección Administrativa	DIRADM2	Rule 21	B2 - B4
Vlan 33	Dependencia Jurídica	JURIDICO	Rule 22	B4 - B5
Vlan 34	Jefatura	JEFATURA1	Rule 23	B5
Vlan 35	Jefatura	JEFATURA2	Rule 24	B5
Vlan 36	Dirección de Intereses Nacionales	INTNAC	Rule 25	B5
Vlan 37	Dirección de Desarrollo Institucional	DESAINST	Rule 26	B5 - B6
Vlan 38	Dirección de Operaciones	DIROPE	Rule 27	B6
Vlan 39	Cooperación Interinstitucional	COOPINTER	Rule 28	B6
Vlan 40	Dirección de Doctrina	DOCTRINA	Rule 29	B6
Vlan 41	Dirección de Planes y Ordenes	PLANORD	Rule 30	B6
Vlan 42	Federación Deportiva	FEDDEP	Rule 31	B6
Vlan 43	Dirección de Comunicación Social	COMSOC	Rule 32	B6
Vlan 44	Dirección de Investigaciones	DIRINV	Rule 33	B7
Vlan 45	Red Wireless	WIRELESS	Rule 34	B4

Fuente: Nancy Yolanda Ramón I.

La configuración de estas reglas está dada de la siguiente manera:

1. Definir el número para la acl avanzada
2. Definir las reglas necesarias

Su configuración es la siguiente:

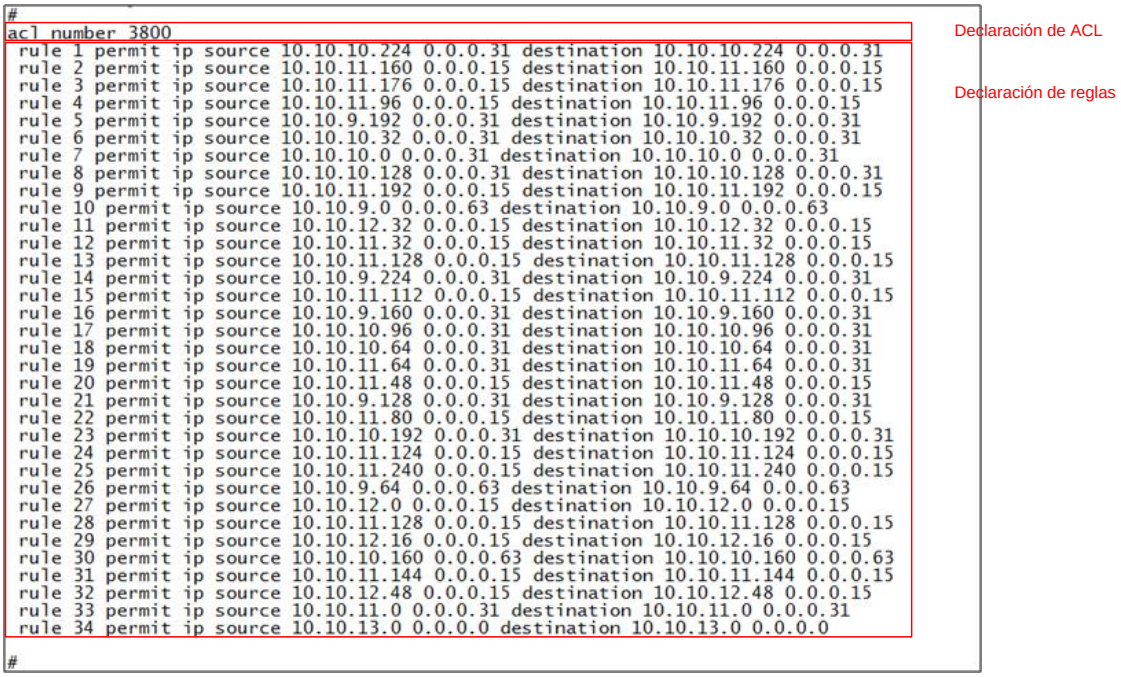


Figura 92. Vista de configuración ACL 3800 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Para que se apliquen los filtros definidos en la lista de acceso 3800 se debe configurar en el puerto trunk del equipamiento activo de manera que el tráfico sea manejado simplemente entre los miembros de una vlan. La declaración de las mismas está dada en función de las vlan que estén configuradas en el equipo.

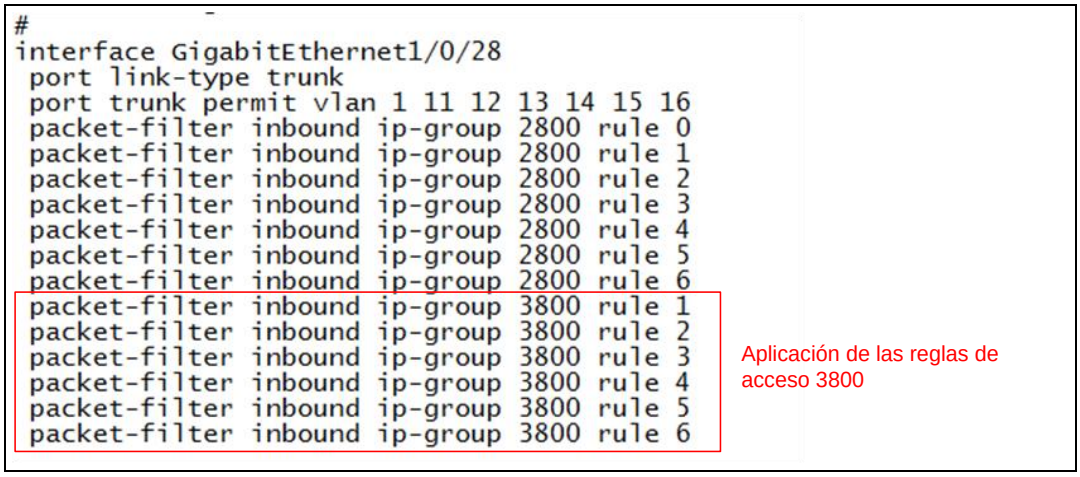


Figura 93. Vista aplicación ACL 3800 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Lista de acceso 2900

Esta lista de acceso limita el acceso remoto para la administración del equipamiento activo a la vlan de los Administradores, a todas las demás redes les niega su acceso. Su configuración debe realizarse de la siguiente manera:

1. Definir el número para la acl básica
2. Definir las reglas necesarias

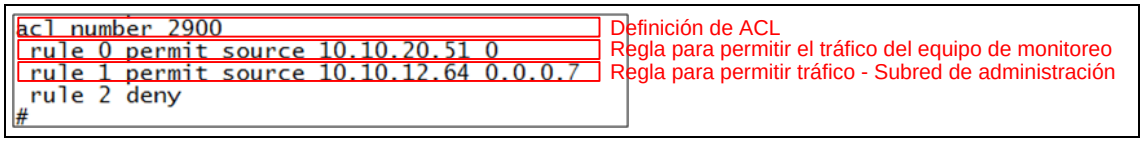


Figura 94. Vista configuración ACL 2900 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Para limitar el acceso remoto la acl 2900 debe ser aplicada en la interface vty de cada switch de la siguiente manera:

1. Ingresar a la interfaz vty
2. Aplicar la acl para el tráfico de entrada

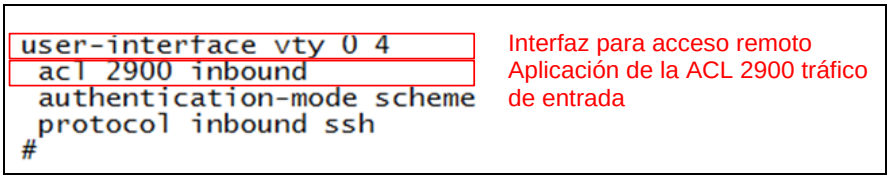


Figura 95. Vista configuración interfaz vty - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

4.3.2.2.6 Configuración de agregados de enlace

La configuración de agregados de enlace permite balancear la carga tanto de entrada como de salida además de brindar estabilidad a la conexión, en función de la carga manejada se debe considerar habilitar la configuración en los equipos de conmutación.

Para su configuración los puertos miembros del grupo deben contener las mismas configuraciones básicas, así también estos deben pertenecer a la misma unidad física.

La configuración debe ser aplicada en los dos equipos en base al siguiente procedimiento:

1. Habilitar LACP en cada uno de los puertos
2. Crear el grupo de agregación de enlace
3. Agregar cada interface al grupo definido

4.3.2.2.7 Configuración de apilamiento de equipos

Para evitar la configuración de equipos en cascada, es importante la aplicación de la tecnología XRN, la cual permite que se maneje a múltiples dispositivos como una sola unidad de red. Es importante tener en cuenta que para apilar los equipos deben tener la misma versión de SO y utilizar el mismo sysname, adicional a la siguiente configuración.

1. Configurar el modo de operación de los puertos SFP en ambos equipos
2. Configurar en el primer equipo el ID de la unidad y el nombre
3. Configurar en el segundo equipo el ID de la unidad en modo autonumérico

```
#
 fabric-port GigabitEthernet1/0/50 enable
 undo xrn-fabric authentication-mode
#
```

Figura 96. Vista configuración XRN unidad 1 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

```
#
 fabric-port GigabitEthernet2/0/51 enable
 fabric-port GigabitEthernet2/0/52 enable
 undo xrn-fabric authentication-mode
#
```

Figura 97. Vista configuración XRN unidad 2 - Capa Acceso

Fuente: Consola de Administración Remota – 3Com

Luego de realizadas las configuraciones respectivas para cada una de las capas del modelo de acuerdo a los criterios detallados en el capítulo 3, la red se encuentra completamente operativa, además en la misma se tienen aplicados criterios de alta disponibilidad, flexibilidad, escalabilidad y seguridad. Adicionalmente se han limitado los dominios de broadcast en función de un análisis amplio sobre la red en estudio.

Es importante tener en cuenta que luego de realizarse la reconfiguración completa del equipamiento a fin de que se ajuste a los requerimientos de diseño, los trabajos referentes al mantenimiento, gestión y administración de la infraestructura de red se facilitan dado que la red del modelo está basada en una infraestructura jerárquica. Al contar con la información actualizada del estado de la red, el administrador cuenta con las herramientas necesarias para la toma de decisiones. Sin embargo es importante tener en cuenta que toda infraestructura de red necesita ser monitoreada de manera que se cuente con una herramienta que muestre en tiempo real su estado. Como un aporte adicional se ha implementado una infraestructura de monitoreo basada en software libre denominada Nagios.

Nagios es una aplicación para el monitoreo tanto de sistemas como de redes, permite verificar el estado de los equipos y servicios que se definan por parte del administrador de red, obteniendo alertas cuando existan problemas y cuando ellos se normalicen.

Además de realizar el monitoreo a la infraestructura de red, este software permite ser configurado por el administrador de manera que se realice la monitorización de los servidores incluyendo el uso de disco, memoria, procesador, entre otros.

Éste software al ser exequible por medio de una interfaz web provee al administrador de una herramienta de fácil uso. En la figura 98 se muestra la pantalla con el detalle de estado de los host monitoreados.

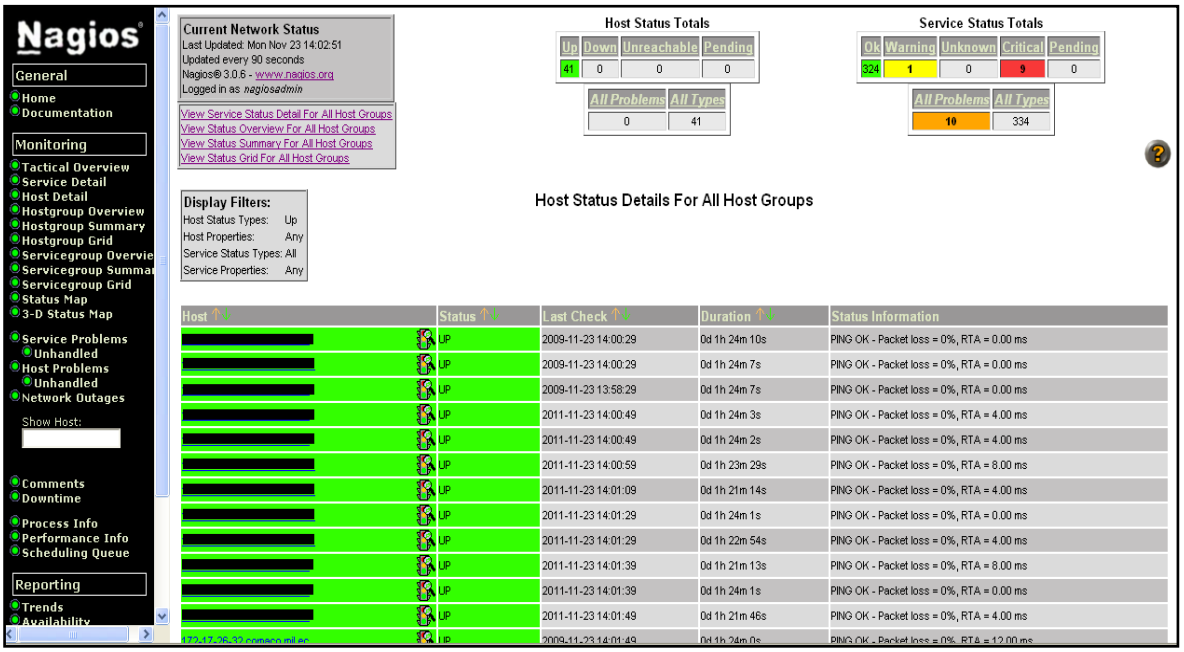


Figura 98. Detalle de estado de host

Fuente: Software de Monitoreo Nagios.

4.4 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.

Al inicio de éste capítulo se muestran las configuraciones realizadas en equipamiento marca 3Com, dado que el equipamiento utilizado en la Institución es

de dicha marca; sin embargo en esta parte se indicarán las principales configuraciones realizadas en tecnología cisco con la cual se demuestre la funcionalidad del modelo propuesto. Como se muestra en el desarrollo de las simulaciones, la sintaxis utilizada por ambos fabricantes es distinta, sin embargo la funcionalidad es la misma. Cabe destacar que en lo que respecta a seguridad a nivel de acceso a la red, los fabricantes manejan una lógica diferente para cada caso.

En vista de que en la primera parte de éste capítulo se realizó un análisis de las configuraciones por cada una de las capas de manera que se tenga clara la funcionalidad de cada una de ellas junto a las configuraciones para cada caso en tecnología 3Com, en esta parte se describirá las configuraciones realizadas según aplique para cada equipo en las diferentes capas, pero no se volverá a explicar su funcionalidad ya que como se indicó anteriormente la sintaxis es la que cambia pero el objetivo de las configuraciones realizadas están dadas en base a un mismo fin.

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 de 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 y ACL basadas en puertos. En cambio el switch 3560 es un switch capa 3, puertos Fast Ethernet y Giga Ethernet, soporta RSTP, 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 24. Características equipamiento Cisco [66]

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
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	-	-

4.4.1 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.

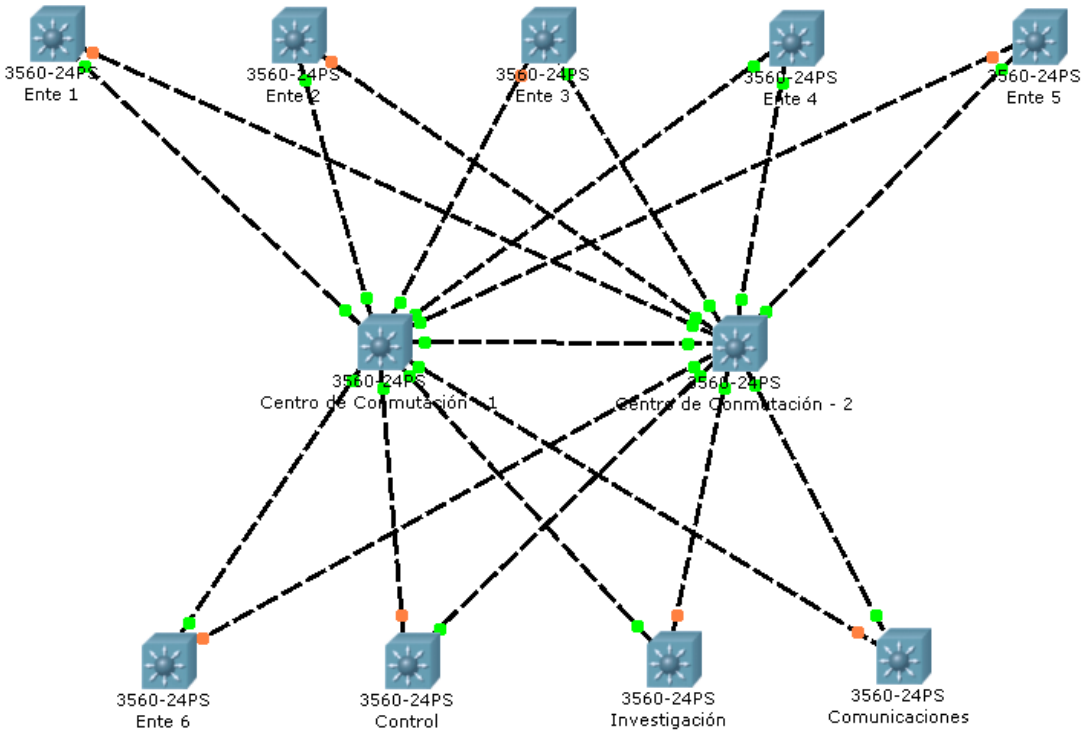


Figura 99. Topología en Alta Disponibilidad

Fuente: Software Packet Tracer version 5.3.1.

La figura 99 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.

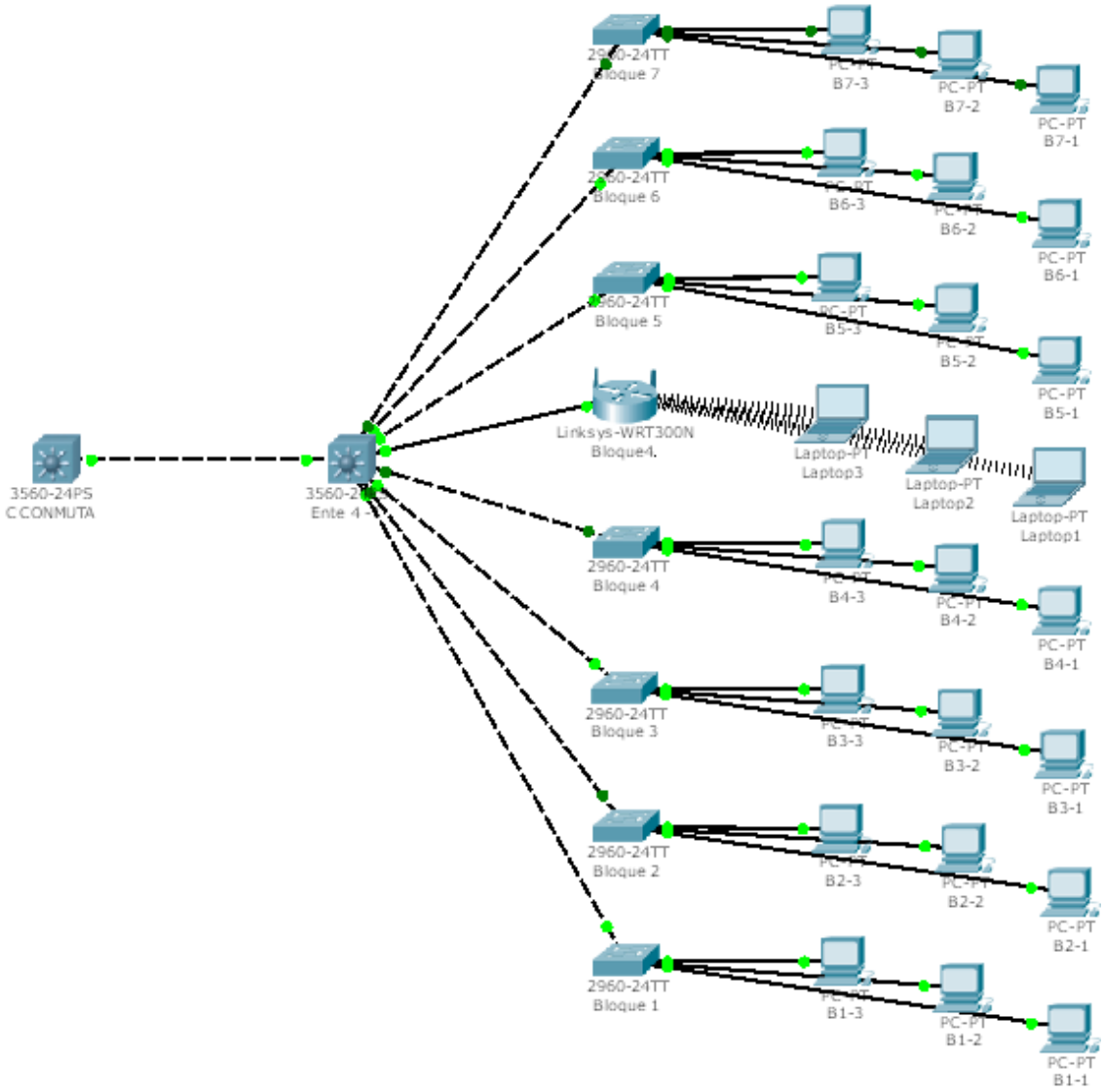


Figura 100. Topología de la red de datos de la Institución

Fuente: Software Packet Tracer version 5.3.1

Para el desarrollo de las configuraciones se tomó como base los datasheet[94] del equipamiento.

4.4.2 CONFIGURACIONES BÁSICAS

En los equipos con tecnología cisco se manejan tres modos de comandos: el modo exec de usuario identificado por el carácter “>”, el modo exec privilegiado identificado por el carácter “#” y el modo de configuración que se habilita mediante el comando “*configure terminal*” dentro del cual se permite configurar el

[94] Tomados de la página oficial de Cisco http://www.cisco.com

equipamiento. En función del modo en el cual se trabaje se manejan diferentes niveles de acceso.

4.4.2.1 Configuración de contraseñas de acceso

Dado que con el modo exec privilegiado se permite realizar cambios en la configuración, es necesario que éste sea protegido por una contraseña de acceso. Así también para proteger el acceso hacia el equipamiento de red se deben configurar las contraseñas para el acceso a la consola y el acceso telnet habilitado por defecto.

Para establecer la contraseña de consola escribir lo siguiente:

- Line console 0
  - Password *contraseña*
  - Login

Una vez establecida la contraseña para la línea de consola, para acceder a la misma se pedirá la contraseña de acceso, como se muestra a continuación:

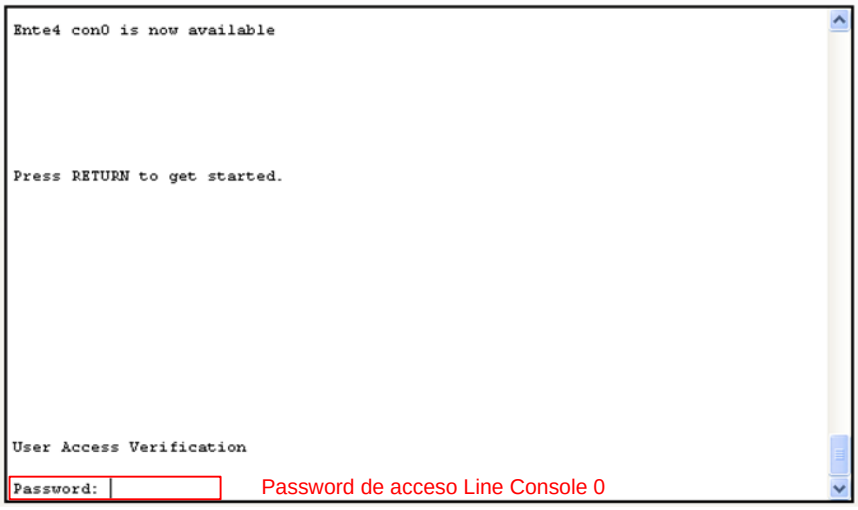


Figura 101. Habilitación contraseña de Línea de Consola

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Para establecer la contraseña para modo exec privilegiado escribir:

- Enable secret *contraseña*

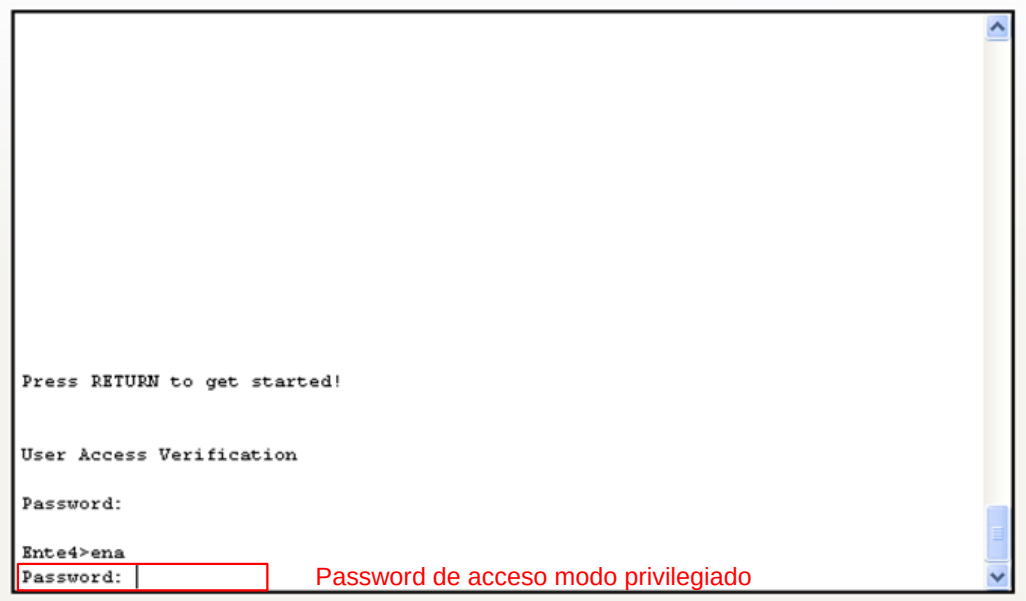


Figura 102. Habilitación modo EXEC privilegiado

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Esta contraseña por defecto se almacenará cifrada

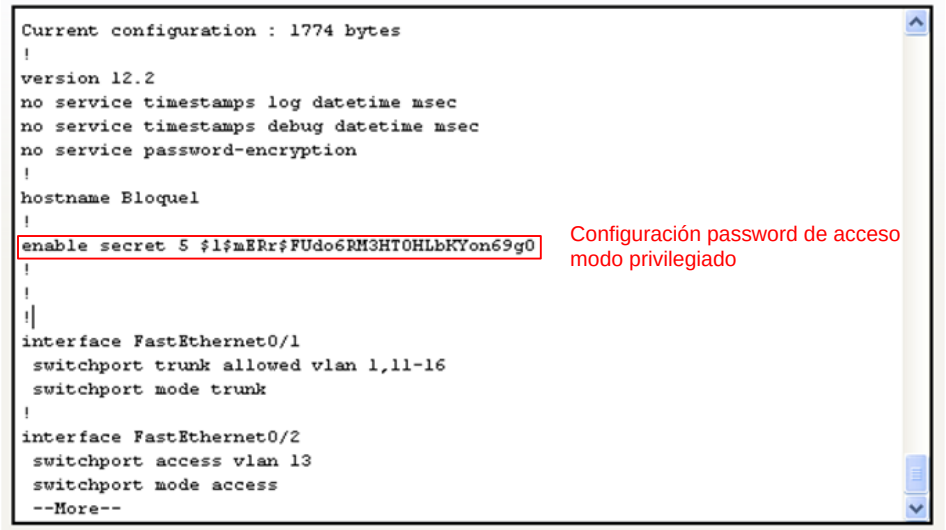


Figura 103. Vista almacenamiento contraseña modo EXEC privilegiado

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Para establecer la contraseña para accesos por el terminal virtual telnet, seguir el siguiente procedimiento:

- Line vty 0 4
  - Password *contraseña*
  - Login

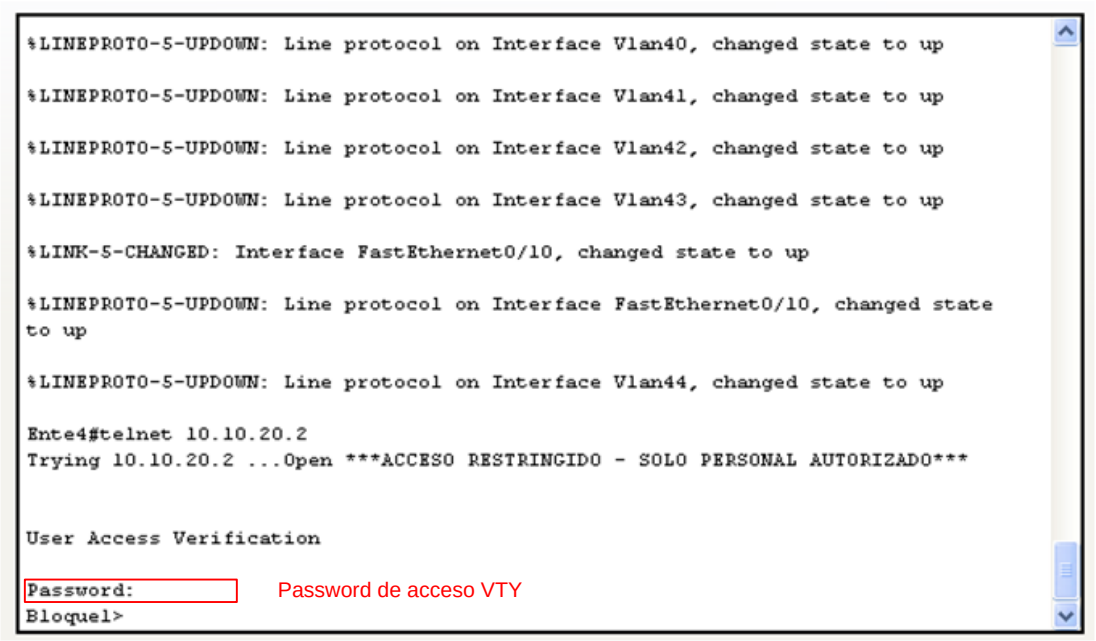


Figura 104. Habilitación contraseña acceso VTY

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

En la siguiente figura se muestra el detalle de las configuraciones realizadas:

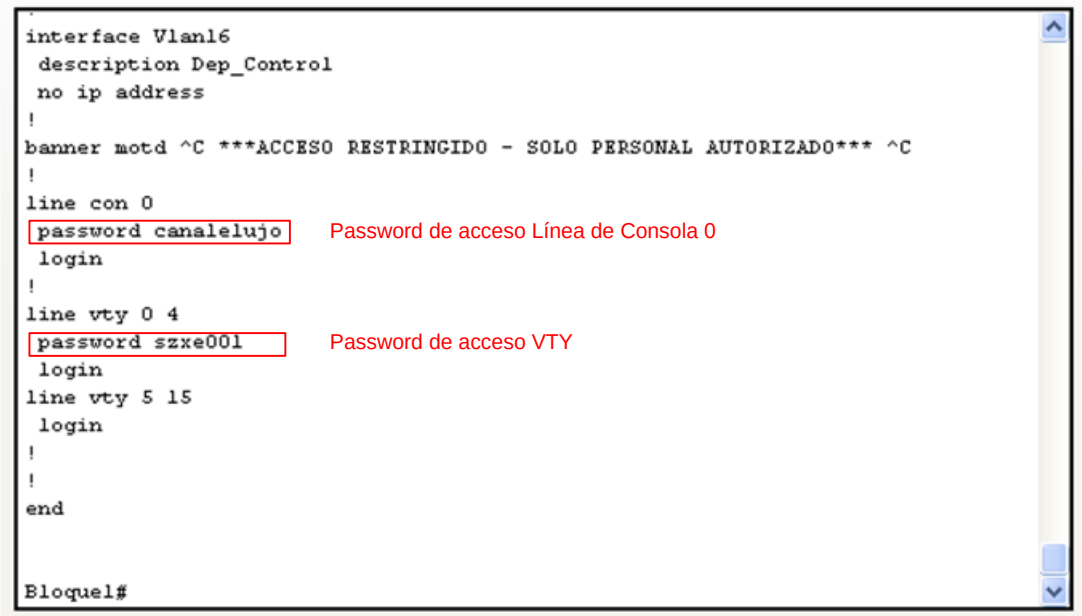


Figura 105. Vista Configuración de contraseñas de acceso

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Es importante tener en cuenta que las contraseñas de acceso creadas no se guardan de manera cifrada por lo cual se debe utilizar la siguiente línea de configuración:

- Service password-encryption

Una vez aplicado el comando antes indicado las contraseñas se almacenarán de manera cifrada, como se muestra en la siguiente figura:

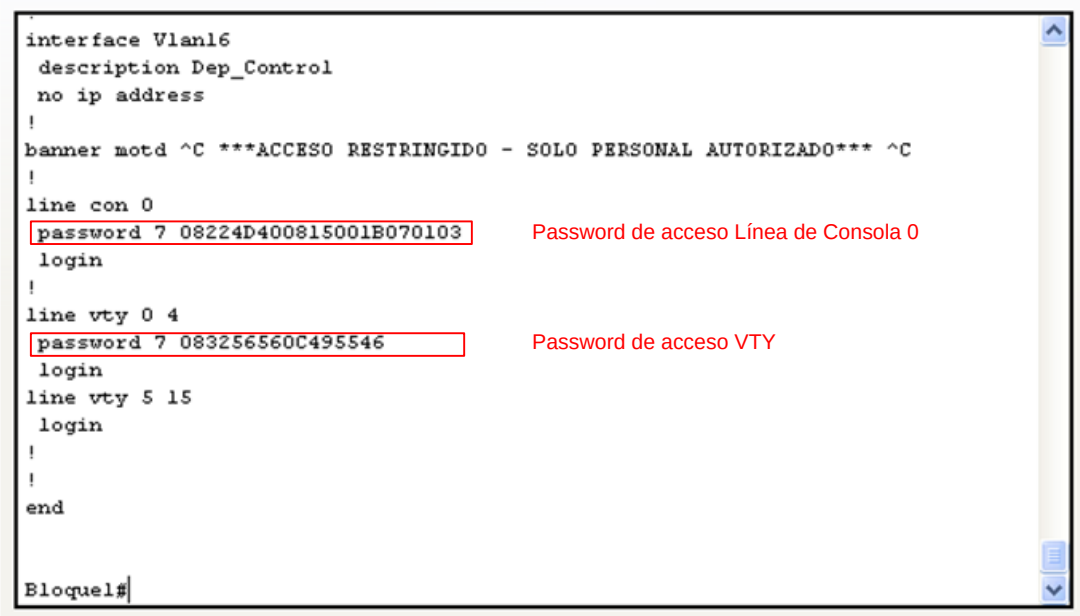


Figura 106. Vista de configuración de contraseñas de acceso cifradas

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

4.4.2.2 Configuración de la dirección IP del equipo

La configuración de la dirección IP del equipo permite administrar de manera remota al equipo. Esta configuración se la ha realizado en la vlan 90 destinada para la administración del equipamiento.

El direccionamiento IP asignado para cada uno de los equipos está dado de la siguiente manera:

Tabla 25. Direccionamiento IP equipamiento activo

Nombre del Equipo	Dirección IP	Máscara	Ubicación
SW_CCONMUTA	10.51.10.49	255.255.255.248	Centro Conmutación
SW_ENTE4	10.51.10.50 10.10.20.1	255.255.255.248 255.255.255.240	TC - Datacenter
SW_BLOQUE1	10.10.20.2	255.255.255.240	TR – Bloque1
SW_BLOQUE2	10.10.20.3	255.255.255.240	TR – Bloque2
SW_BLOQUE3	10.10.20.4	255.255.255.240	TR – Bloque3
SW_BLOQUE4	10.10.20.5	255.255.255.240	TR – Bloque4

SW_BLOQUE5	10.10.20.7	255.255.255.240	TR – Bloque5
SW_BLOQUE6	10.10.20.8	255.255.255.240	TR – Bloque6
SW_BLOQUE7	10.10.20.9	255.255.255.240	TR – Bloque7

Fuente: Nancy Yolanda Ramón I.

Para su configuración seguir los siguientes pasos:

1. Ingreso a la interfaz de administración Vlan 90
2. Asignar la dirección IP de administración del equipo.

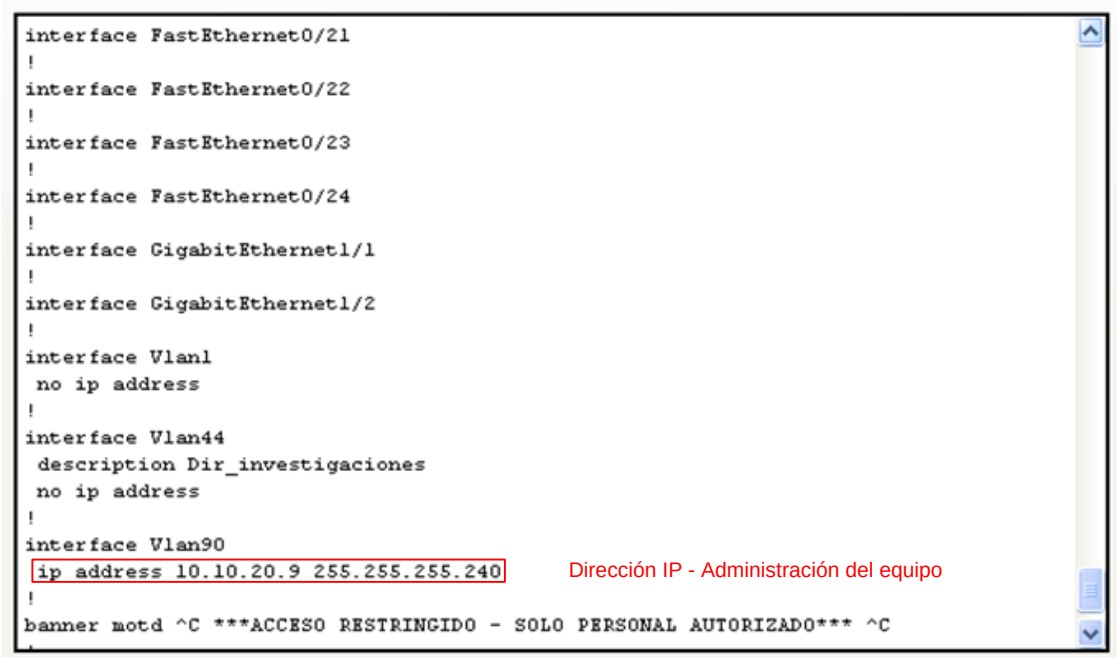


Figura 107. Configuración de la IP de administración

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Luego de configurada la dirección IP en cada uno de los equipos se cuenta por defecto con el acceso remoto tipo telnet:

Para su acceso se debe utilizar la contraseña configurada en el terminal vty.

4.4.2.3 Configuración del nombre del equipo

La definición del nombre del equipo facilita las tareas de administración del mismo, su configuración se la realiza de la siguiente manera:

- Hostname *nombre_equipo*

4.4.2.4 Configuración de acceso SSH[95]

Antes de habilitar el acceso SSH es necesario que se configure el nombre del equipo y se defina un nombre de dominio, lo cual servirá como base para la generación de la clave RSA.

1. Configuración del nombre del dominio
    - ip domain-name *midena.local*
2. Generación de las claves RSA
    - crypto key generate rsa
3. Especificar el número de bits que se utilizarán, por defecto se encuentra establecido en 512 : *1024*
4. Definición del tiempo de time out de ssh
    - ip ssh time-out 30
5. Definición de los reintentos de validación permitidos
    - ip ssh authentication-retries 2
6. Definición de la versión de ssh
    - ip ssh version 2
7. Definición del usuario y contraseña permitidos para el acceso vía ssh y sus privilegios:
    - username root privilege 15 password canalelujo1102
8. Aplicar la habilitación de ssh para el terminal virtual
    - line vty 0 4
9. Activar ssh
    - transport input ssh
10. Definir método de logueo.
    - login local

[95] SSH: *Secure Shell*

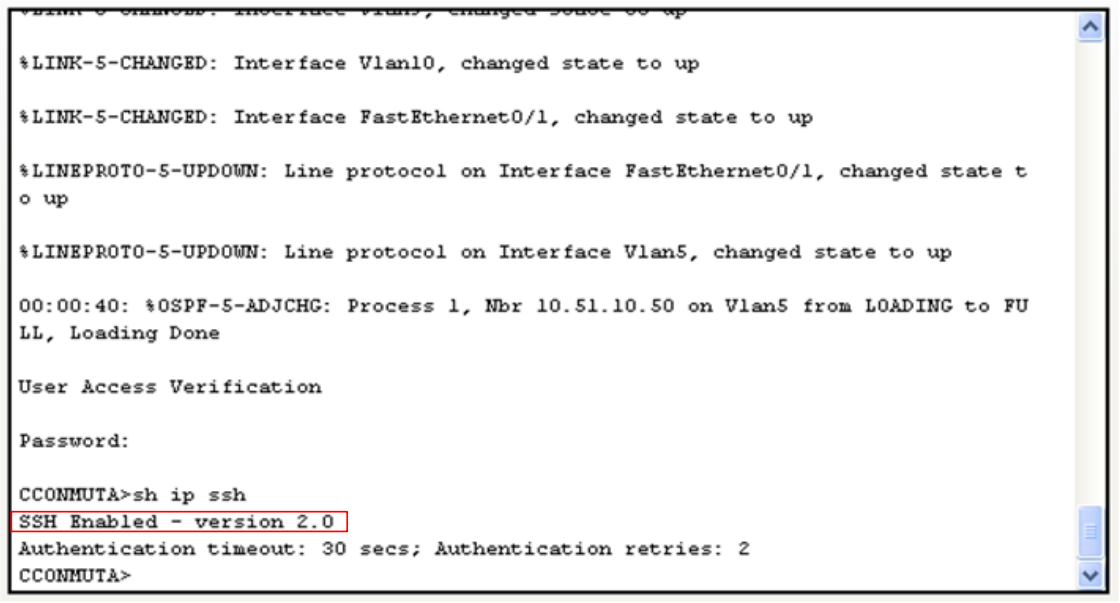


Figura 108. Vista configuración protocolo SSH

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

Para validar el acceso SSH desde un PC, ingresar el nombre de usuario y la dirección IP del equipo remoto, como se muestra a continuación.

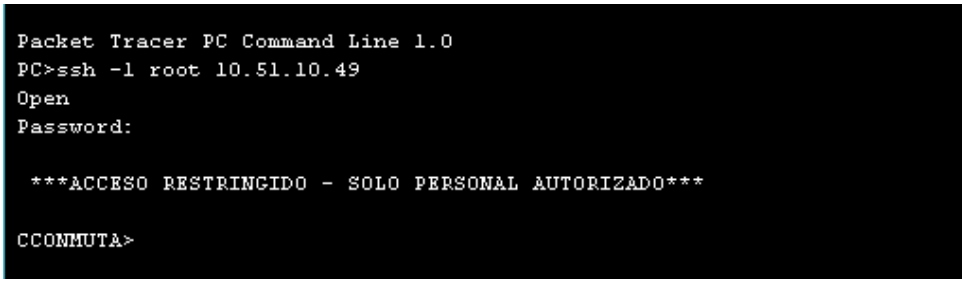


Figura 109. Vista acceso SSH

4.4.2.5 Configuración de banners de bienvenida

Para configurar los banners de bienvenida escribir el siguiente comando:

- Banner motd c *mensaje_de_bienvenida* c

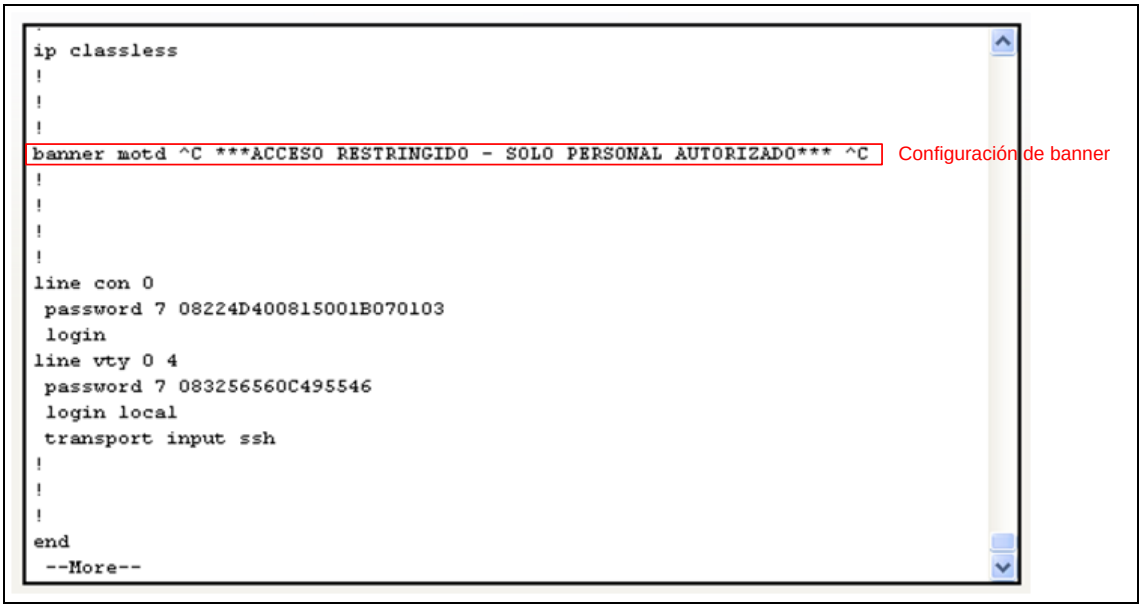


Figura 110. Vista configuración de banner

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

4.4.3 CONFIGURACIÓN DE VLAN

La configuración de las vlan están dadas en base a la tabla 21, los pasos a seguir para realizar dicha configuración son las siguientes:

- Declarar la vlan en función del id
- Definir el nombre de la vlan
- Agregar la descripción de la vlan definida

Los pasos 2 y 3 son opcionales, sirven para facilitar las tareas de administración.

Luego de declaradas las vlan en el caso de los switches de núcleo y distribución se debe asignar la dirección IP de la vlan, para ello seguir los siguientes pasos.

- Ingresar a la interfaz de la vlan
- Asignar el direccionamiento IP correspondiente
- Asignar la descripción a la interfaz de la vlan

Las configuraciones desarrolladas se muestran en las siguientes figuras:

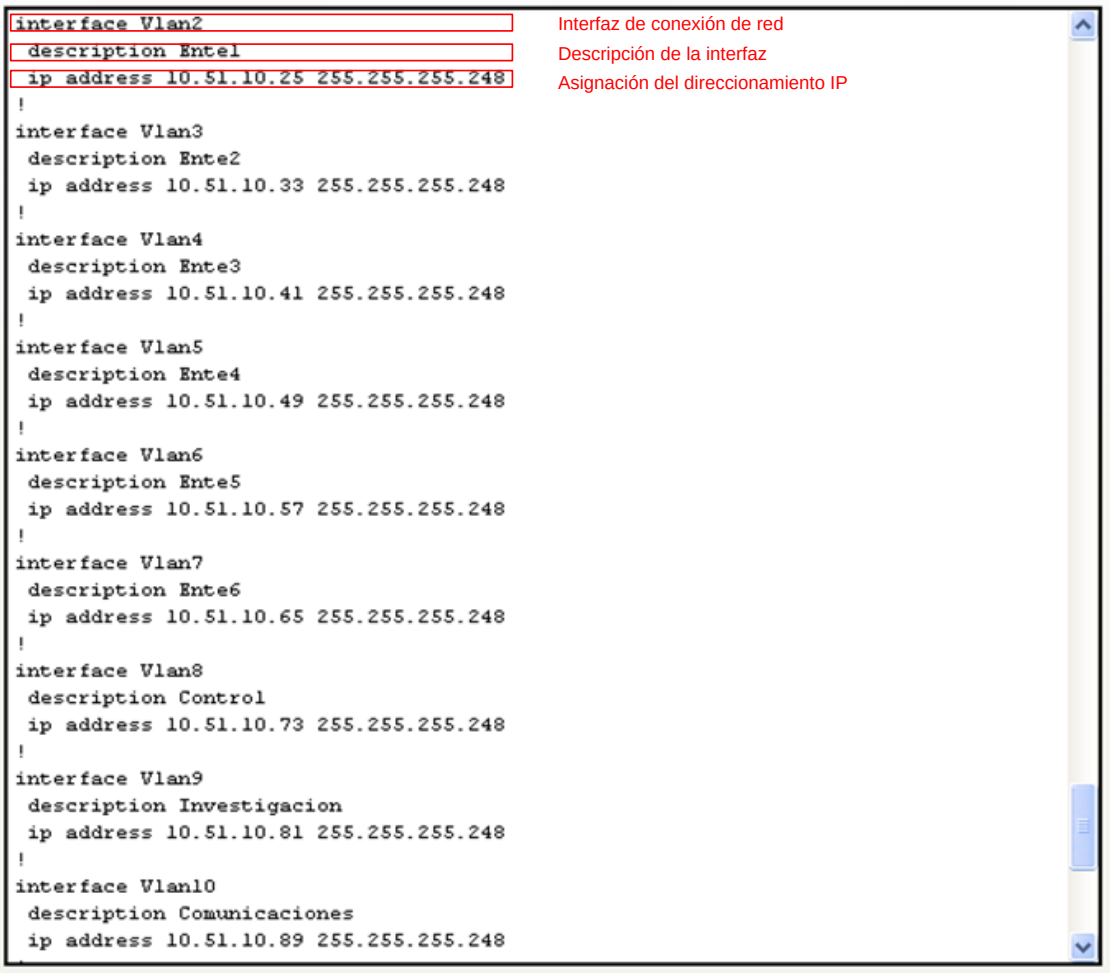


Figura 111. Configuración de vlan a nivel de núcleo – Sw CCONMUTA

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

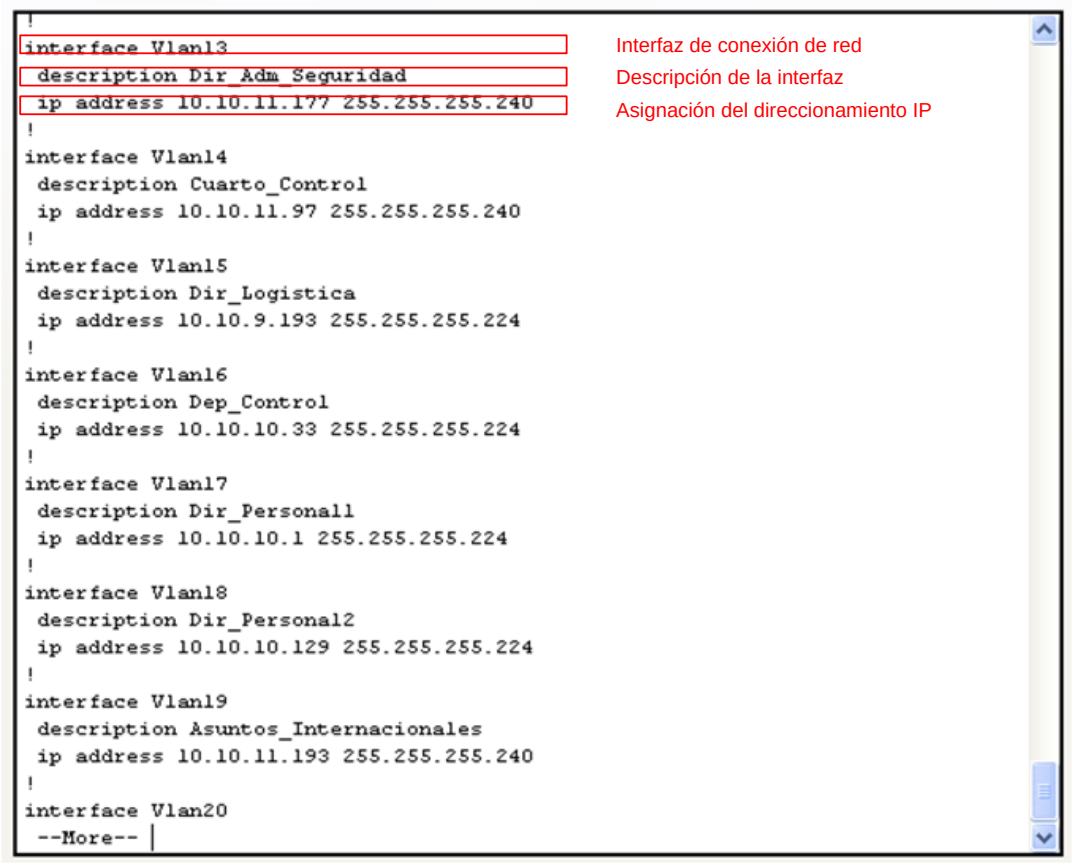


Figura 112. Configuración de vlan a nivel de distribución – Sw Ente4

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

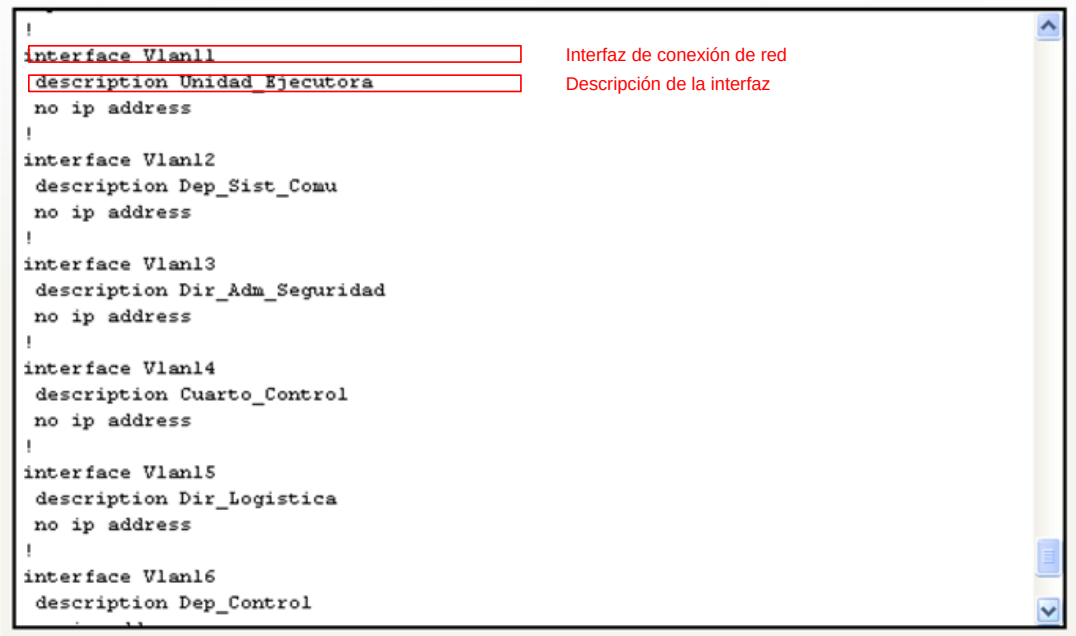


Figura 113. Configuración de vlan a nivel de acceso – Sw Bloque1

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

4.4.4 CONFIGURACIÓN DE PUERTOS

Una vez que se han definido las vlan correspondientes se puede asignar las mismas a los puertos que conciernan. Para esto es importante diferenciar los puertos que deben asignarse en modo trunk y los que deben asignarse en modo acceso.

- Puerto conectado hacia una PC – puerto tipo acceso
- Puerto conectado hacia un servidor - puerto tipo acceso
- Puerto conectado hacia otro switch con una vlan - puerto tipo acceso
- Puerto conectado hacia otro switch con varias vlan - puerto tipo trunk

La configuración de puertos tipo trunk está dada de la siguiente manera:

- Ingresar a la interfaz del puerto deseado
- Designar el puerto en modo trunk
- Seleccionar la encapsulación dot1q
- Configurar las vlan asociadas al puerto

La configuración de puertos tipo acceso está dada de la siguiente manera:

- Ingresar a la interfaz del puerto deseado
- Designar el puerto en modo acceso
- Establecer la vlan a la cual pertenece el puerto

La configuración realizada es la siguiente:

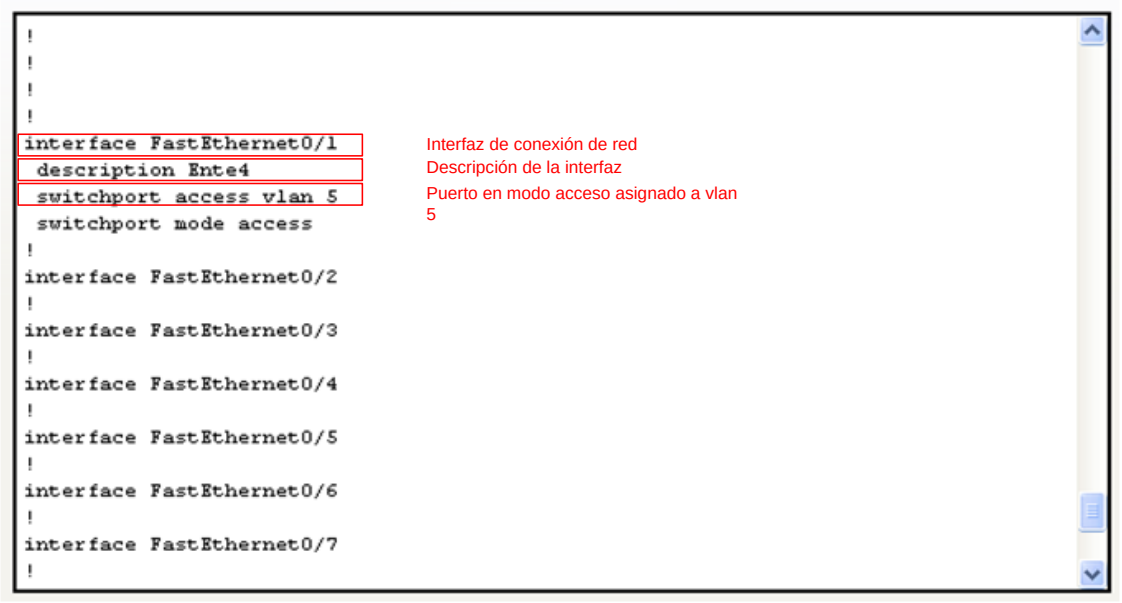


Figura 114. Configuración de interfaces a nivel de núcleo - Sw CCONMUTA

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

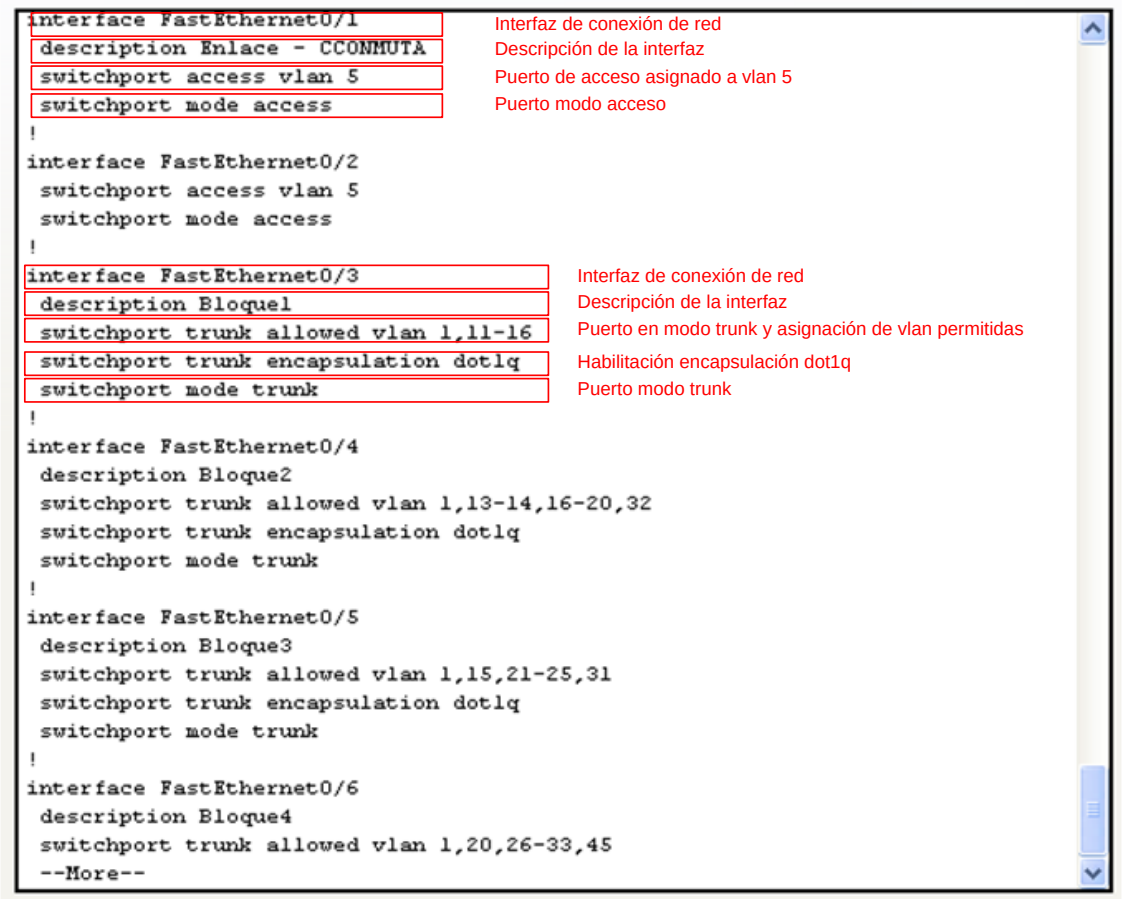


Figura 115. Configuración de interfaces a nivel de distribución - Sw Ente4

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

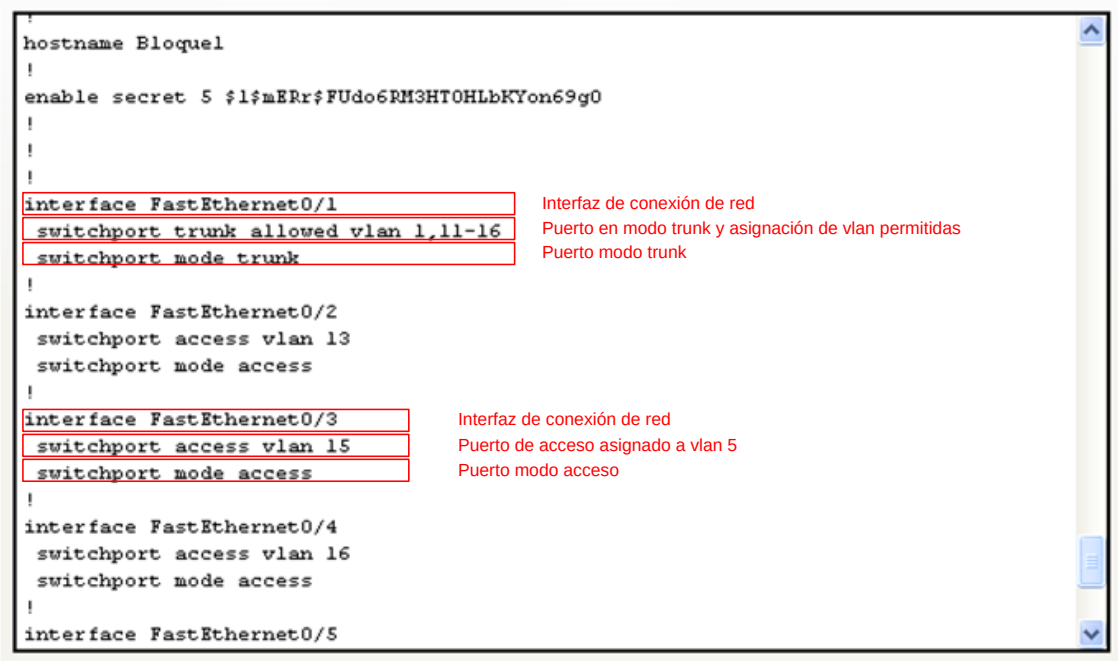


Figura 116. Configuración de interfaces a nivel de acceso - Sw Bloque1

Fuente: Nancy Yolanda Ramón I.

4.4.5 CONFIGURACIÓN DEL PROTOCOLO OSPF

Mediante la configuración del protocolo OSPF se permite habilitar un tipo de enrutamiento dinámico, establecido como estándar en la entidad. Para su configuración se debe seguir lo siguientes pasos:

- Establecer el tipo de enrutamiento ospf
- Definir las redes que se encuentran conectadas directamente al equipo y el área a la que pertenecen

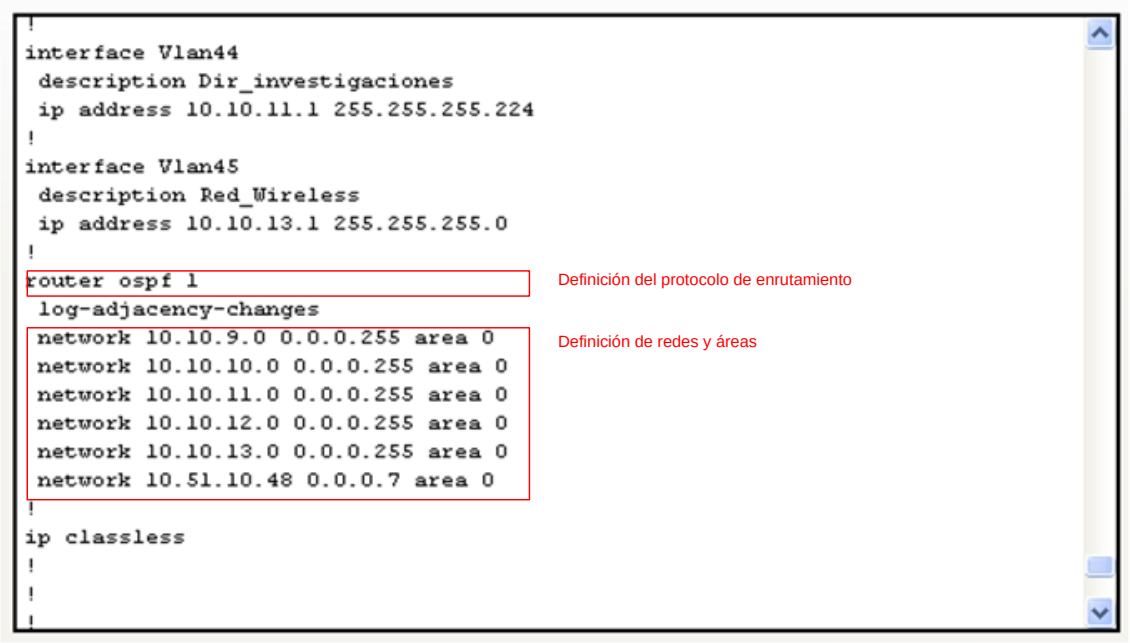


Figura 117. Configuración protocolo OSPF a nivel de distribución - Sw Ente4

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

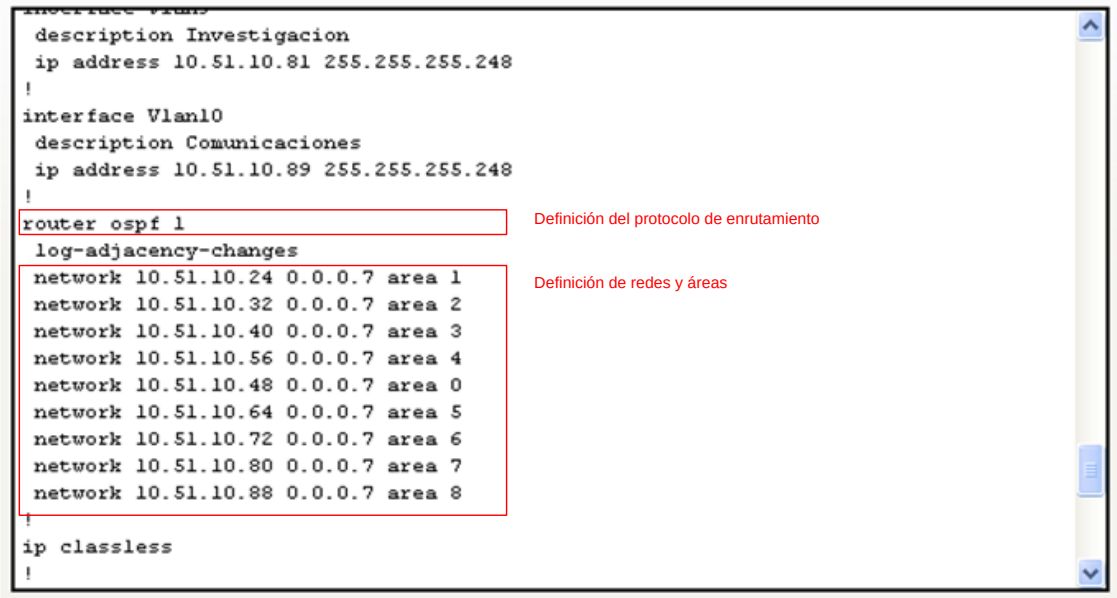


Figura 118. Configuración protocolo OSPF a nivel de núcleo - Sw CCONMUTA

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

4.4.6 HABILITACIÓN DE ALTA DISPONIBILIDAD – PROTOCOLO SPANNING TREE

Con el protocolo spanning tree se permite crear una topología libre de bucles, esto lo realiza deshabilitando los enlaces redundantes y levantando los mismos

sólo en caso de ser necesario, es decir cuando el enlace principal no se encuentre activo. En su configuración es importante definir el equipo que manejará como root, permitiendo definirse en base a la prioridad manejada. La configuración realizada se muestra a continuación:

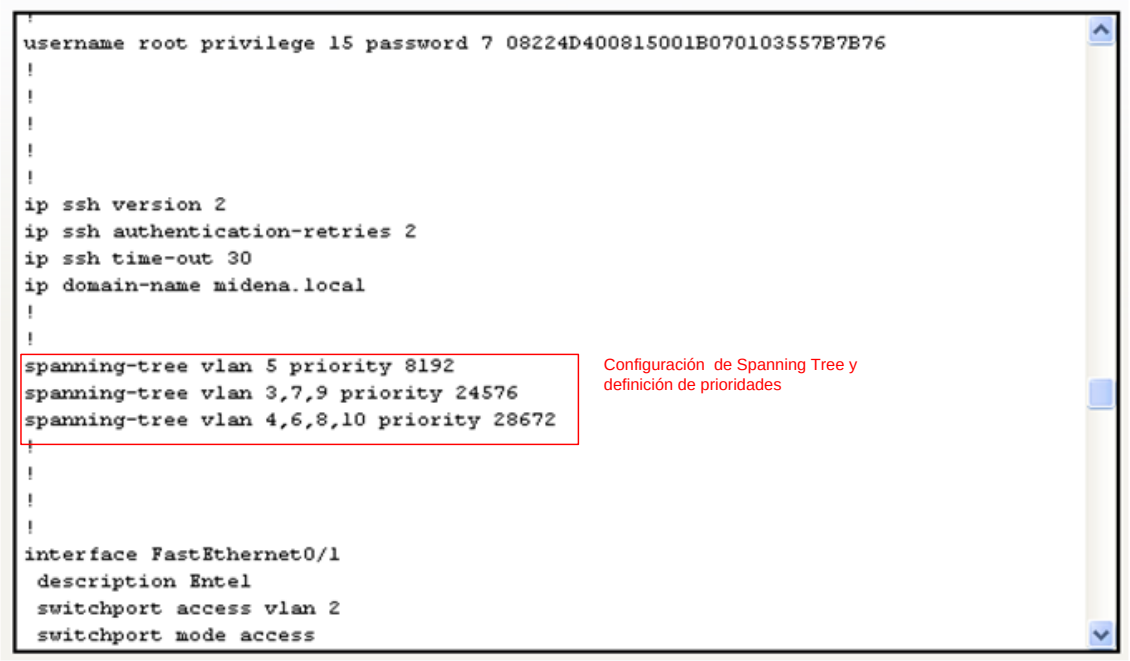
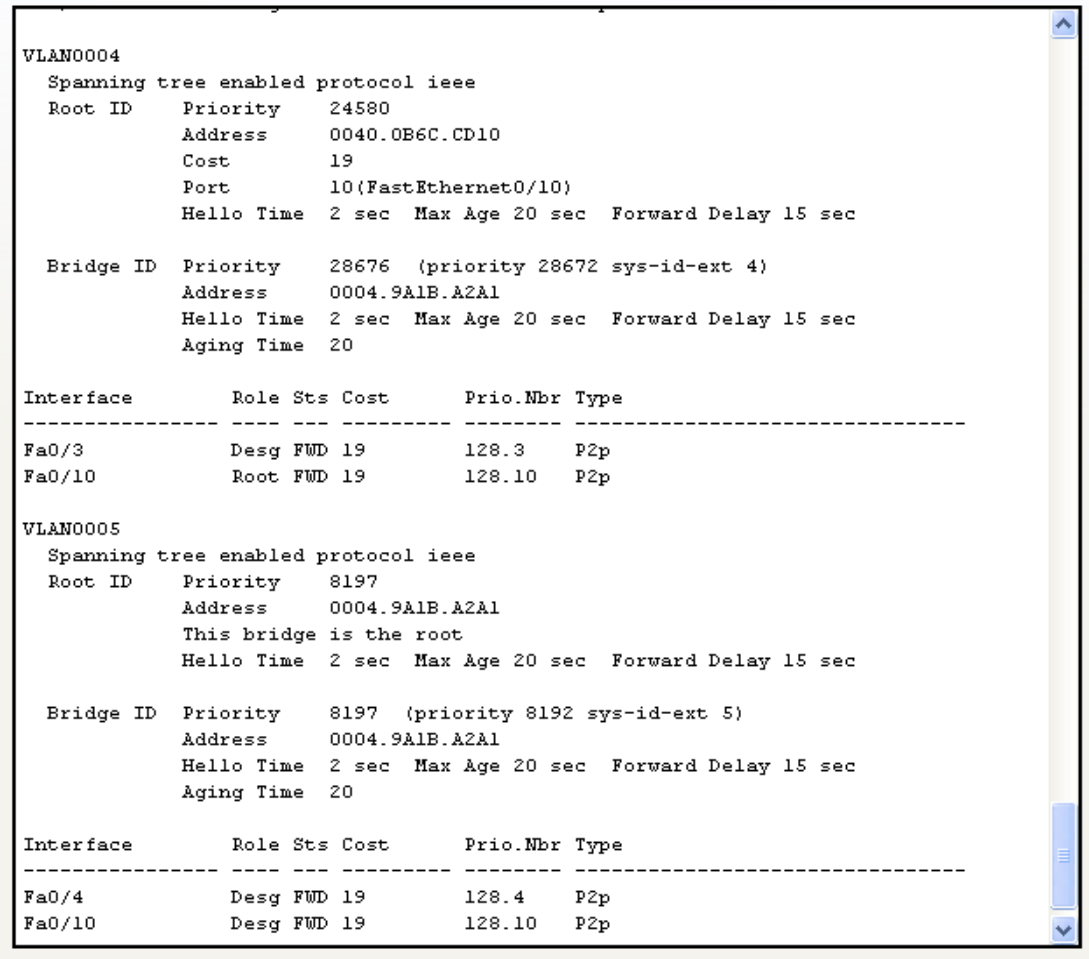


Figura 119. Vista configuración de prioridades en Spanning Tree

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1



```
VLAN0004
  Spanning tree enabled protocol ieee
  Root ID     Priority    24580
              Address     0040.0B6C.CD10
              Cost        19
              Port        10(FastEthernet0/10)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28676  (priority 28672 sys-id-ext 4)
              Address     0004.9A1B.A2A1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/10           Root FWD 19        128.10   P2p

VLAN0005
  Spanning tree enabled protocol ieee
  Root ID     Priority    8197
              Address     0004.9A1B.A2A1
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    8197  (priority 8192 sys-id-ext 5)
              Address     0004.9A1B.A2A1
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/10           Desg FWD 19        128.10   P2p
```

Figura 120. Vista configuración de Spanning Tree

Fuente: Configuración equipos - Software Packet Tracer version 5.3.1

4.5 OBJETIVOS FUNCIONALES

4.5.1 SEGURIDAD

Uso de contraseñas para limitar el acceso local y remoto.- dado que mediante al acceso a la configuración del terminal se accede a 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:- 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 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.

4.5.2 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. En las figuras se muestra el caso del envío de un paquete cuando se cuenta con toda la infraestructura activa uno de los puertos del enlace se encuentra en estado de espera, cuando uno de los enlaces falla toma el control el segundo enlace y se procede a enviar los mismos por la nueva ruta asignada para la entrega del paquete.

Habilitación protocolo de Spanning Tree.- La 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.

4.5.3 ESCALABILIDAD

Manejo 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.

4.5.4 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. Así también su administración se facilita.

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.

4.5.4 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, ni rendimiento a nivel de aplicación.

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.

CAPITULO 5. CONCLUSIONES Y RECOMENDACIONES

En base al desarrollo del trabajo realizado, en éste capítulo se exponen las principales conclusiones y recomendaciones a tomar en cuenta para la implementación y administración de la red de Datos de la Institución.

5.1 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. Así también 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 y la necesidad del servicio brindado hacia los diferentes Entes del Ministerio de Defensa por medio de la red de Datos, la aplicación de un modelo redundante tanto a nivel de enlaces como de equipamiento hace que la red cuente con alta disponibilidad asegurándose la continuidad del servicio, tanto a nivel de red interna como externa.

- El estudio de la infraestructura de red permitió identificar a detalle las principales fortalezas y falencias de la red, mediante las cuales se determinó el modelo adecuado para cumplir los objetivos funcionales del mismo, utilizando la infraestructura de red existente en función de sus características y prestaciones.

- Mediante la certificación de puntos de red realizada en la institución se determinó el estado del cableado estructurado a nivel de recorridos horizontales, encontrándola operativa en su mayor parte. Su certificación fue de fundamental importancia dado que es necesario primero determinar el estado del canal físico para luego asegurar el canal de comunicación,

permitiendo brindar el servicio de manera adecuada. Teniendo en cuenta que de los puntos que no pasaron la certificación la mayor parte fue debido a problemas en el mapa de cableado, entre el 50 y 70% de ellos ya fueron solucionados brindando a la red una mayor cantidad de puntos operativos.

- La aplicación de microsegmentación a nivel de acceso reduce el alcance de los dominios de broadcast al segmentar la red en pequeños grupos asociados en base a funciones, roles y recursos compartidos, además brinda mayor seguridad al tener acceso simplemente entre los usuarios de la vlan y de ser el caso con usuarios que necesiten realizar tareas especificas con los usuarios de otra vlan, caso contrario el tráfico entre usuarios de diferentes vlan estará cerrado; también posee flexibilidad al permitir que los usuarios de manera independiente de su ubicación física formen parte de su vlan de acceso.

- Con el levantamiento de información realizado a nivel de usuarios, se entrega a la institución la documentación técnica que servirá de ayuda en las tareas de administración y gestión, adicionalmente el administrador contará con la información necesaria para la toma de decisiones, teniendo en cuenta que el levantamiento de información a nivel de cableado estructurado, equipamiento activo, disponibilidad de puertos y servidores es de vital importancia para el manejo de la red, operación y mantenimiento.

- La aplicación de seguridad a nivel de puerto con el uso del control basado en IP y MAC Address asegura que solo las máquinas autorizadas e inventariadas dentro de la red de la institución tengan acceso hacia la red interna, además brinda al administrador el control sobre la misma dado que se evitan problemas ocasionados por el cambio o robo de direcciones IP.

- La aplicación del nuevo modelo de etiquetamiento para los puntos de red permitirá al administrador de red conocer de manera exacta el número del punto de red, la ubicación en patch panel, el servicio prestado además del Bloque al cual se brinde el servicio, facilitando tareas de administración, gestión y mantenimiento de la misma.

- El uso de un software para monitoreo de la red permite al administrador actuar de manera proactiva ante fallos en la infraestructura, adicionalmente con la ayuda del mismo tendrá una herramienta de diagnóstico visual que le permita analizar el estado de la red y la toma de decisiones.

- 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.

- Mediante el desarrollo de las configuraciones en equipamiento de tecnología 3Com y la simulación del modelo propuesto en un simulador del mercado se puede 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.

5.2 RECOMENDACIONES

- El personal encargado de la administración y gestión de la red debe estar actualizado y capacitado de forma continua en gestión y administración de redes además en seguridad informática para la toma de decisiones ante problemas y progresos en la red.

- Para todas las instalaciones de cableado estructurado que se realicen, debe utilizarse accesorios y ductos adecuados, además de una correcta identificación, teniendo en cuenta los criterios detallados en las normas ANSI/TIA/EIA.

- Se recomienda llevar una bitácora de todos los acontecimientos presentados en la red, tanto los incidentes producidos como las acciones que se tomen al respecto.

- Se debe documentar todos los cambios que se realicen en la red, tanto a nivel de usuarios, enlaces, direccionamiento aplicado, vlan asignada, perfiles, entre otros, de manera que se cuente con la información actualizada y en cualquier momento se pueda tomar decisiones en base a ella. Esta documentación facilitará las tareas de administración en caso de que el personal encargado no se encuentre presente y se deba delegar funciones.

- Es importante que se establezcan políticas a nivel de red de manera que se regule y controle el uso de ella y de los equipos computacionales, la misma que luego de ser aprobada debe ser socializada a todo el personal de la institución de manera que se dé cumplimiento al mismo.

- En vista de que el Data Center constituye un punto crítico en la red interna es importante que este cuente con un constante monitoreo en tiempo real, con el uso de cámaras de seguridad, además es importante contar con un monitoreo digital que alerte al administrador ante la presencia de valores anormales en el ambiente del mismo.

- Para la aplicación del modelo que brinde alta disponibilidad a la red, se debe tomar en cuenta rutas diferentes para la instalación de los enlaces de conexión, de manera que de producirse falla en el recorrido del enlace, el canal alterno no se vea afectado y se asegure la continuidad del servicio.

- Se debe contar con procedimientos para el cambio periódico de contraseñas del equipamiento activo, utilizando contraseñas con un nivel de complejidad adecuado, utilizando la combinación de letras mayúsculas, minúsculas, números y caracteres especiales de manera que se brinde mayor seguridad a la misma; dentro del procedimiento deben considerarse el mecanismo para el almacenamiento bajo custodia de las contraseñas cambiadas, en caso de que las mismas sean requeridas de manera

urgente y ningún personal de la sección se encuentre en el establecimiento. Estas contraseñas sólo podrán ser abiertas en situaciones extremas por el Jefe de la sección.

- Se recomienda realizar backup periódicos de las configuraciones del equipamiento activo, guardando las versiones anteriores (mínimo 5), de manera que de ocurrir problemas en alguna configuración mal aplicada o corrupción de la misma se pueda subir un backup y restituir de manera inmediata el servicio. En dependencia del cambio de configuraciones a nivel de equipamiento se recomienda sacar backup semanales o quincenales dados mediante un procedimiento establecido.

- Con el fin de precautelar la seguridad de la institución y tener un control sobre los equipos computacionales y el uso de los mismos, es conveniente que todos los equipos sean configurados dentro del directorio activo institucional.

- El software de monitoreo debe ser constantemente revisado, además se debe tener en cuenta que cualquier cambio o adición que se realice en la infraestructura debe ser actualizado en el mismo.

- Dado que el proyecto se basa en la aplicación de seguridad a nivel de red, es importante que se apliquen soluciones firewall para brindar seguridad a la red perimetral ante accesos no autorizados u ataques a la misma.

- Se deben implementar esquemas técnicos de seguridad perimetral para la red de internet y de datos tales como Firewall, IDS, IPS, VPN.

- Se recomienda que los puertos del equipamiento de red que no estén siendo utilizados con autorización del personal de administración sea deshabilitado, de manera que se controle y regule el uso de la red asegurando además su seguridad.

- De los problemas detectados a nivel de puntos finales de cableado estructurado es importante que se trate de dar solución a los que por problemas de mal manejo o prácticas de instalación presentan fallas en el

mapa de cableado en alguno de sus extremos, sin embargo los puntos de red con problemas internos del cable, de preferencia no deben ser utilizados ya que la eficiencia del enlace no está garantizada.

CAPÍTULO 5

REFERENCIAS BIBLIOGRÁFICAS

[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.mitecnologico.com/Main/AntecedentesHistoricosRedes

[18] http://www.bbn.com/about/timeline/arpanet

[19] http://www.nic.funet.fi/index/FUNET/history/internet/en/arpanet.html

[20] http://www.darpa.mil/

[21] http://www.isoc.org/

[22] http://www.oocities.org/fisiclady1/lab5AnalogtoDigitalConverter.pdf

[23] http://www.mitecnologico.com/Main/Se%F1alesAnalogicasYDigitales

[24] http://www.textoscientificos.com/redes/comunicaciones/modos

[25]http://www.mitecnologico.com/Main/TecnicasDeTransmisionSincronaYAsincrona

[26] http://ariadna.ii.uam.es/wiki/wiki_ar1/doku.php?id=la_capa_fisica

[27] http://www.alfinal.com/Temas/bandaancha.php

[28] http://aritzgaiarre.blogspot.com/2009/11/limitaciones-del-ancho-de-banda.html

[29] http://redesfundamento.blogspot.com/

[30]http://atcj.wordpress.com/page/2/

[31] http://www.robertoares.com.ar/wp-content/uploads/2010/06/Seccion-3.pdf http://www.versatek.com/

[32] http://www.bloginformatico.com/topologia-de-red.php

[33] http://www.mitecnologico.com/Main/TopologiasDeRed

[34] http://www.angelfire.com/mi2/Redes/topologia.html

[35]http://www.cuentame.inegi.gob.mx/museo/cerquita/redes/fundamentos/03.htm

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

[37]http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf----vlan

[38] http://www.unsa.edu.pe/infounsa/cursor/01/cursor01.pdf

[39] http://es.kioskea.net/contents/internet/vlan.php3

[40] http://elies.rediris.es/elies18/321.html

[41] http://www.ieee.org/index.html

[42] http://www.ietf.org/

[43] http://www.iso.org/iso/home.html

[44] http://www.itu.int/es/pages/default.aspx

[45] http://esp.hyperlinesystems.com/catalog/cable/

[46]http://www.profesores.frc.utn.edu.ar/electronica/ElectronicaAplicadaIII/PlantelExterior/Introducables.pdf

[47] http://www.cablewire.es/

[48]http://www.commserv.ucsb.edu/infrastructure/standards/history/EIA-TIA_568.asp

[49] http://tutorial.galeon.com/inalambrico.htm

[50] http://www.alfinal.com/Temas/fibraoptica.php

[51] http://www.monografias.com/trabajos12/reina/reina.shtml

[52] http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

[53] http://www.elrinconcito.com/articulos/Sesiones/sesiones.pdf

[54] http://www.mitecnologico.com/Main/ModosDeTransmision

[55] http://www.dte.us.es/personal/mcromero/docs/arc1/tema2-arc1.pdf

[56] http://www.ansi.org/

[57]http://www.rfc-es.org/rfc/rfc1918-es.txt

[58] http://www.ecaus.org/eia/site/index.html

[59] http://www.alfinal.com/Temas/cableadoestructurado.php

[60]http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/CableadoEstructurado2.pdf

[61]http://www.tiaonline.org/standards/

[62] http://www.luguer.com/catalogos/pdf/DTX_ES.pdf

[63] http://www.flukenetworks.com/datacom-cabling/copper-testing/LinkWare-Stats

[64] http://h17007.www1.hp.com/us/en/index.aspx

[65] http://www.fingertec.com/images/w_brochure/AC900_e.html

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

ÍNDICE DE ACRÓNIMOS

ACL: Access Control List (Listas de Control de Acceso)

ACR: Attenuation/Crosstalk Ratio (Relación Atenuación-Diafonía)

ADSL: Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica)

AP: Access Point (Punto de Acceso)

ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)

ARPA: Advanced Research Proyects Agency (Agencia de Investigación de Proyectos Avanzados)

ARPANET: Advanced Research Proyects Agency Network (Red de la Agencia de Investigación de Proyectos Avanzados)

ASIC: Application-Specific Integrated Circuit (Circuitos Integrados de Aplicación Específica)

BGP: Border Gateway Protocol (Protocolo de Gateway de Borde)

BITNET: Because It's Time Network (Red Porque ya es Hora)

BPDU: Bridge Protocol Data Units (Unidad de Datos de Protocolo Puente)

CE: Cableado estructurado

CHAP: Challenge Handshake Authentication Protocol (Protocolo de Autenticación por Desafío Mutuo)

CNLP: Connection less Network Layer Protocol (Protocolo de Capa de Red Sin Conexión)

CPU: Central Processing Unit (Unidad Central de Procesos)

CSMA/CD: Carrier Sense Multiple Access with Collision Detection (Acceso Múltiple por Detección de Portadora con Detección de Colisiones

CSNET: Computer Science Network (Red de Ciencias de la Computación)

DES: Data Encryption Standard (Estándar de Cifrado de Datos)

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)

DNS: Domain Name System (Sistema de Nombres de Dominio)

EAPOL: Extensible Authentication Protocol Over LAN (Protocolo de Autenticación Ampliable sobre LAN)

ECMP: Equal-Cost Multi-Path (Igual Costo Multitrayecto)

EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Gateway Interior Mejorado)

ELFEXT: The Equal-Level Far-End Crosstalk (Telediafonía por igualación de Nivel)

FEXT: Far-End Crosstalk (Interferencia de Extremo Lejano - Telediafonía)

FTP: Foiled Twisted Pair (Par Trenzado con Pantalla Global)

FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)

HTTPS: Hypertext Transfer Protocol Secure (Protocolo de Transferencia de Hipertexto Seguro)

ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

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

IETF: Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet)

IGMP: Internet Group Management Protocol (Protocolo de Administración de Grupos de Internet

IGRP: Interior Gateway Routing Protocol (Protocolo de Ruteo de Gateway Interior

IMAP: Internet Message Access Protocol (Protocolo de Acceso a Mensajes Internet)

IP: Internet Protocol (Protocolo de Internet)

IPX: Internetwork Packet Exchange (Intercambio de Paquetes Interred)

IS-IS: Intermediate System - Intermediate System (Sistema Intermedio - Sistema Intermedio)

ISM: Industrial, Scientific and Medical (Industrial, Científica y Médica)

ISO: International Standards Organization (Organización Internacional de Estándares)

ITU: International Telecomunication Union (Unión Internacional de Telecomunicaciones)

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

LAN: Local Area Network (Redes de Área Local)

LLC: Control de Enlace Lógico (Logical Link Control)

LSP: Link State PDU (PDU de Estado de Enlace)

MAC: Media Access Control (Control de Acceso al Medio)

MAN: Metropolitan Area Network (Red de Área Metropolitana)

MAPs: Managed Access Points (Administración de Puntos de Acceso)

MILNET: Military Network (Red Militar)

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

NEXT: Near-End Crosstalk (Interferencia de Extremo Cercano)

NIC: Network Interface Card (Tarjeta de Interfaz de Red)

ODFs: Optical Distribution Frame (Repartidores de Fibra Óptica)

OSI: Open System Interconnection (Interconexión de Sistemas Abiertos)

OSPF: Open Shortest Path First (Primero el Camino Libre más Corto)

PAP: Password Authentication Protocol (Protocolo de Autenticación de Contraseña)

PIM SM/DM: Protocol Independent Multicast Sparse Mode/Dense Mode (Protocolo Multicast Independiente Modo Esparcido/Modo Denso)

PoE: Power Over Ethernet (Poder sobre Ethernet)

POP: Post Office Protocol (Protocolo de la Oficina de Correo)

PSELFEXT: Power Sum the Equal-Level Far-End Crosstalk (Telediafonía de Suma de Potencias por Igualación de Nivel)

PSNEXT: Power Sum Near-End crosstalk (Paradiafonía de Suma de Potencias)

QoS: Quality of Service (Calidad de Servicio)

RARP: Reverse Address Resolution Protocol (Protocolo de Resolución de Dirección Inversa)

RIP: Routing Information Protocol (Protocolo de Información de Enrutamiento)

RSN: Robust Secure Network (Red de Seguridad Robusta)

RSTP: Rapid Spanning Tree Protocol (Protocolo Rápido de Spanning Tree)

SCE: Sistema de Cableado Estructurado

SMTP: Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)

SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)

SPF: Shortest Path First (Primero la Ruta más Corta)

SSH: Secure Shell (Intérprete de Comandos Seguro)

SSID: Service Set IDentifier (Identificador de Conjunto de Servicio)

STP: Shielded Twisted Pair (Par Trenzado Apantallado)

STP: Spanning Tree Protocol (Protocolo de Spanning Tree)

TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)

TCP/IP: Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet)

TELNET: Telecommunication Network (Red de Telecomunicaciones)

TIC: Tecnologías de la Información y Comunicación

TKIP: Temporal Key Integrity Protocol (Protocolo de Integridad de Clave Temporal)

TSB: Technical Service Bulletin (Boletín Técnico de Servicio)

UDP: Protocolo de Datagrama de Usuario (User Datagram Protocol)

UPS: Uninterruptible Power Supply (Fuente de Alimentación Ininterrumpible)

UTM: Unified Threat Management (Gestión Unificada de Amenazas)

UTP: Unshielded Twisted Pair (Cable Trenzado sin Apantallar)

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

VLSM: Very Large Mask Variable (Máscara de Longitud Variable)

WAN: Wide Area Network (Red de Área Extensa)

WAP: Wireless Application Protocol (Protocolo de Aplicaciones Inalámbricas)

WEP: Wired Equivalent Privacy (Privacidad Equivalente por Cable)

WIFI: Wireless Fidelity (Fidelidad inalámbrica)

WLAN: Wireless Local Area Network (Redes de Área Local Inalámbricas)

WPA: Wifi Protect Access (Acceso Inalámbrico Protegido)

XRN: eXpandable Resilient Networking (Networking Redundante Expansible)

ANEXOS

ANEXO 1. *DISTRIBUCIÓN DE PUNTOS DE RED*

BLOQUE 1						
IP:	**10.10.9.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.9.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.9.10	Cuarto de Control	Administrador	Punto de red en malas condiciones	CD	3	PASA
10.10.9.16	Departamento de Sistemas	Operador		D1-13	13	PASA
10.10.9.17	Departamento de Sistemas	Operador		D1-10	10	PASA
10.10.9.18	Departamento de Sistemas	Supervisor		D1-18	18	PASA
10.10.9.19	Centro de Telecomunicaciones	Jefe de seguridad		D1-04	1	PASA
10.10.9.23	Logística Bodega	Abastecimiento		D1-02	2	PASA
10.10.9.41	Unidad Ejecutora	Oficial de Ingeniería	AP sw Wireless	D1-21	21	PASA
10.10.9.42	Unidad Ejecutora	Oficial de Ingeniería		D1-23	23	PASA
10.10.9.43	Unidad Ejecutora	Oficial de Ingeniería		D1-24	24	PASA
10.10.9.44	Unidad Ejecutora	Oficial de Ingeniería	Cambio de Face Plate	D1-25	5	PASA
10.10.9.50	Dirección Administrativa	Supervisor		D1-28	8	PASA
	Centro de Telecomunicaciones		Libre	D1-39	voz	PASA
	Centro de Telecomunicaciones		Libre	D1-08	.	PASA
10.10.9.55	Departamento de Comunicaciones	Jefatura		D1-06	6	PASA
	Centro de Telecomunicaciones		Libre	D1-38	.	PASA
	Centro de Telecomunicaciones		Libre	D1-07	.	PASA
	Centro de Telecomunicaciones		Libre	D1-05	.	PASA
	Central Telex		Libre	D1-40	.	PASA
	Central Telex		Libre	D1-17	.	PASA
	Central Telex		Libre	D1-42	.	PASA
	Central Telex		Libre	D1-16	.	PASA
	Central Telex	Fax	Fax	D1-15	voz	PASA
	Central Telex		Libre	D1-41	.	PASA
	Central Telex		Libre / Sin etiquetar	D1-43	.	PASA

	Central Telex		Libre	D1-44	.	PASA
	Central Telex		Libre	D1-45	.	PASA
	Sección Datotex		Libre	D1-14	.	PASA
10.10.9.31	Sección Datotex	Operador	Sin etiquetar	D1-46	voz	PASA
	Sección Datotex		Libre	D1-47	.	PASA
10.10.9.35	Sección Datotex	Operador	Cámara IP	D1-12	17	PASA
	Sección Radio		Libre	D1-11	.	PASA
	Sección Radio		Libre	D1-48	.	PASA
	Unidad Ejecutora		Libre/Sin etiquetar	D1-22	.	PASA
	Policía Militar		Libre	D1-27	.	FALLA
	Sala de Breafing		Libre	D1-19	.	PASA
	Sala de Breafing		Libre/Suelto cajetín	D1-20	.	PASA
10.10.9.61	Departamento de Comunicaciones	Adm. Lectores de Huellas	Cable Directo	V2-30	14	PASA
10.10.9.62	Departamento de Comunicaciones	Adm. Lectores de Huellas	Cable Directo	V2-31	15	PASA
10.10.9.65	Departamento de Comunicaciones	Operador		D1-26	.	FALLA
10.10.9.67	Departamento de Comunicaciones	Secretaría		V1-39	4	PASA
10.10.9.37	Unidad Ejecutora	Operador	Sin etiquetar	V1-26	7	PASA
10.10.9.56	Dirección Administrativa	Operador	Sin etiquetar	V1-29	12	PASA
10.10.9.57	Unidad Ejecutora	Supervisor		ALIM. AP	.	NO CERT
10.10.9.68	Unidad Ejecutora	Técnico Sección		ALIM. AP	.	NO CERT
10.10.9.69	Unidad Ejecutora	Técnico Sección		ALIM. AP	.	NO CERT

BLOQUE 2						
IP:	**10.10.10.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.10.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.10.9	Salón Auditorio	Auditorio		D1-22	24(1)	PASA
10.10.10.10	Dirección de Personal	Director		D2-10	8(2)	PASA
10.10.10.11	Dirección de Personal	Secretaría Director		D2-20	33(2)	PASA
10.10.10.12	Dirección de Personal	Subdirector		D2-09	7(2)	PASA
	Dirección de Personal	Secretaría	Libre	D2-07	.	PASA
10.10.10.14	Dirección de Personal	Derechos Humanos		D1-48	48(1)	PASA
10.10.10.15	Dirección de Personal	Supervisor		D2-03	3(2)	PASA
	Dirección de Personal	Fuerza de Tarea	Voz	D1-46	Voz	PASA
10.10.10.18	Dirección de Personal	Pases		D1-47	47(1)	PASA
10.10.10.20	Dirección de Personal	Estadística		D2-01	4(2)	PASA
10.10.10.21	Dirección de Personal	Tec. De Archivo		D1-39	39(1)	PASA
10.10.10.22	Dirección de Personal	Sec. Técnica		D1-36	36(1)	PASA
10.10.10.23	Dirección de Personal	Jefe de Jefatura		D1-37	37(1)	PASA
10.10.10.24	Dirección de Personal	Analista RRHH		D1-38	38(1)	PASA
10.10.10.25	Dirección de Personal	Analista Financiero		D1-30	30(1)	PASA
10.10.10.26	Dirección de Personal	Tec. Nomina		D1-31	31(1)	PASA
10.10.10.27	Dirección de Personal	Ast. RRHH		D1-32	32(1)	PASA
10.10.10.28	Dirección de Personal	Oficinista		D1-33	33(1)	PASA
10.10.10.29	Dirección de Personal	Ast. Administrativo		D1-34	34(1)	PASA
10.10.10.30	Dirección de Personal	Trabajadora Social		D1-19	19(1)	PASA
10.10.10.31	Dirección de Personal	Permisos		D1-43	43(1)	PASA
10.10.10.32	Dirección de Personal	Sec. Servicio Social	Sin Etiqueta	D1-17	16(1)	FALLA
10.10.10.34	Dirección de Personal	Bienestar Psicología		D1-16	11(1)	PASA
10.10.10.36	Dirección de Personal	Jefe Dep. Plan Militar		D1-14	14(1)	PASA
10.10.10.38	Dirección de Personal	Amanuense	Sin Etiqueta, Sin Face Plate, Sin canalizaciones	D2-27	17(2)	PASA

10.10.10.39	Dirección de Personal	Escalafón	Sin Etiqueta	D1-45	45(1)	PASA
10.10.10.41	Departamento de Control	Jefe de Departamento		D1-04	4(1)	PASA
10.10.10.42	Departamento de Control	Subjefatura		D2-17	17(1)	PASA
10.10.10.44	Departamento de Control	Sección Técnica	Libre/Sin Etiqueta	D1-03	.	FALLA
10.10.10.45	Departamento de Control	Administrativo	SWITCH	D1-01	1(2)	PASA
10.10.10.47	Departamento de Control	Administrativo		D1-06	14(3)	PASA
10.10.10.55	Asuntos Internacionales	Jefatura		D1-27	27(1)	PASA
10.10.10.56	Asuntos Internacionales	Secretaría		D1-25	25(1)	PASA
10.10.10.57	Asuntos Internacionales	Agregadurías		D1-26	26(1)	PASA
10.10.10.58	Asuntos Internacionales	Agregadurías	SWICTH	D1-29	29(1)	PASA
10.10.10.66	Ingreso de Personal	Inspector Seguridad		D1-20	20(1)	PASA
10.10.10.67	Departamento de Pagaduría	Asistente mensajería		D2-22	22(1)	PASA
10.10.10.69	Departamento de Pagaduría	Tesorería		D2-21	21(1)	PASA
10.10.10.72	Puesto de Mando	Inspector Seguridad	Libre	D2-19	.	PASA
10.10.10.75	Puesto de Mando	Inspector Seguridad		D1-21	23(1)	PASA
	Dirección de Personal		Libre	D1-42	.	PASA
	Cafetería		Libre	D2-02	.	PASA
	Dirección de Personal	Director	Libre	D2-06	.	PASA
	Dirección de Personal	Subdirector	Libre	D2-08	.	PASA
	Dirección de Personal		Libre	D2-12	.	PASA
	Dirección de Personal		Libre	D2-11	.	PASA
	Dirección de Personal		Libre	D2-13	.	PASA
10.10.10.78	Departamento de Planificación	Administrativo		D1-15	15(1)	PASA
10.10.10.79	Departamento de Control	Administrativo		D1-28	38(2)	PASA
	Departamento de Control	Cafetería	Libre	D1-44	.	PASA
	Departamento de Control	Cafetería	Voz/Sin Etiqueta	D1-23	Voz	PASA
	Departamento de Control	Cafetería	Libre	D2-16	.	PASA
	Departamento de Control	Sección Técnica	Voz	D1-02	Voz	PASA
	Departamento de Control	Cafetería	Libre/Sin Etiqueta	D1-05	.	PASA
	Asuntos Internacionales		SW ENCORE 8P	D1-09	.	PASA
	Departamento de Control		Libre	D1-13	13(1)	PASA
10.10.10.80	Departamento de Control	Sala de Sesiones	Cajetín Suelto	D1-12	12(1)	PASA
	Departamento de Control		SW Control de Armas	D1-11	.	PASA

	Ingreso de Personal		Libre	D2-14	.	PASA
	Archivo		Libre	D1-40	.	PASA
10.10.10.82	Departamento de Control	Administrativo		D1-10	10(1)	PASA
10.10.10.83	Departamento de Pagaduría	Administrativo		V2-26	2(1)	PASA
10.10.10.84	Departamento de Pagaduría	Secretaría		V2-27	3(1)	PASA
10.10.10.85	Dirección de Bienestar	Sicóloga		D1-18	18(1)	PASA
10.10.10.86	Dirección de Personal	Ingresos		D1-41	41(1)	PASA
10.10.10.87	Ingreso de Personal	Inspector de Seguridad		D2-26	11(2)	PASA
	Departamento de Pagaduría		Libre	D1-07	.	FALLA
10.10.10.89	Cuarto de Control	Control sistemas personal	Cable Directo al Bloque1	CD	19(2)	PASA
10.10.10.90	Ingreso de Personal	Lectores de huellas	Lectores de Huellas	CD	26(2)	PASA
10.10.10.91	Ingreso de Personal	Lectores de huellas	Lectores de Huellas	CD	27(2)	PASA
	Asuntos Internacionales	Administrativo	Libre	V1-29	.	PASA
	Ingreso Documentación	Secretaría	Libre	D2-25	.	PASA
	Departamento de Control	Director	SW. Control de Armas/Sin Etiqueta	102	1(3)	SIN CERT
	Departamento de Control	Subdirector	SW. Control de Armas/Sin Etiqueta	A5	2(3)	SIN CERT
	Departamento de Control	Secretaría	SW. Control de Armas/Sin Etiqueta	A8	3(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	A12	4(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	V1-15	5(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	A9	6(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	D2-05	7(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	A16	8(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	8	9(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	D1-08	16(3)	SIN CERT
	Departamento de Control	Administrativo	SW. Control de Armas/Sin Etiqueta	A3	15(3)	SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A1		SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A2		SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A4		SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A6		SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A7		SIN CERT
	Departamento de Control		Libre/Sin Etiqueta	A10		SIN CERT

	Departamento de Control		Libre/Sin Etiqueta	A11		SIN CERT

BLOQUE 3						
IP:	**10.10.11.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.11.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.11.9	Dirección de Logística	Sala de Sesiones		D1-45	.	FALLA
10.10.11.10	Dirección de Logística	Director		D1-47	47	PASA
10.10.11.11	Dirección de Logística	Secretaría		D1-44	44	PASA
10.10.11.12	Dirección de Logística	Sub Director		D2-01	25	PASA
10.10.11.13	Dirección de Logística	Subdirección, Amanuense		D1-33	33	PASA
10.10.11.14	Dirección Administrativa	Director		D1-36	36	PASA
	Dirección de Mantenimiento y Transporte	Administrativo	Sin Face plate	D1-24	.	FALLA
10.10.11.16	Dirección Administrativa	Administrativo		D1-35	35	PASA
10.10.11.17	Departamento de Evaluación y Control	Director		D1-32	5	PASA
10.10.11.18	Dirección Administrativa	Secretaría		D1-37	37	PASA
10.10.11.19	Departamento de Evaluación y Control	Administrativo		D1-34	24	PASA
10.10.11.20	Dirección de Logística	Administrativo		D1-28	28	PASA
10.10.11.21	Dirección de Logística	Asesoría Jurídica		D1-31	31	PASA
10.10.11.22	Dirección de Logística	Asesoría Jurídica	Sin etiqueta	D1-30	30	PASA
	Dirección de Logística	Sala de Sesiones		D1-48	.	PASA
	Dirección de Logística	Sala de Sesiones		D1-43	.	PASA
	Dirección de Logística	Sala de Sesiones		D2-02	.	PASA
	Dirección de Logística	Sala de Sesiones		D2-03	.	PASA
10.10.11.23	Cuartel General	Planificación		D1-27	27	PASA

10.10.11.24	Cuartel General	Supervisor		D1-38	32	PASA
10.10.11.25	Cuartel General	Seguros de Vehículos		D1-26	26	PASA
10.10.11.26	Cuartel General	Transportes		D1-23	23	PASA
10.10.11.27	Departamento de Ingeniería	Jefatura		D1-21	21	PASA
10.10.11.29	Departamento de Ingeniería	Obras civiles		D1-20	20	PASA
10.10.11.30	Departamento de Ingeniería	Obras civiles		D1-15	15	PASA
10.10.11.32	Departamento de Ingeniería	Planificación		D1-17	17	FALLA
10.10.11.33	Departamento de Ingeniería	Planificación		D1-18	18	PASA
10.10.11.34	Departamento de Ingeniería	Secretaría		D1-41	41	PASA
10.10.11.35	Departamento de Ingeniería	Secretaría		D1-39	39	PASA
	Departamento de Ingeniería	Libre	Sin etiqueta	D1-40	.	PASA
10.10.11.36	Dirección de Logística	Jefatura	FISICAM	D2-07	42	PASA
10.10.11.37	Dirección de Logística	Administración portal	FISICAM	D2-04	4	PASA
10.10.11.38	Departamento de Contratación Pública	Operador		D2-09	45	PASA
10.10.11.39	Departamento de Contratación Pública	Operador		D2-14	22	PASA
10.10.11.40	Departamento de Contratación Pública	Libre		D2-08	.	PASA
10.10.11.41	Departamento de Contratación Pública	Administrativo	Sin Jack	D2-15	40	PASA
10.10.11.42	Departamento de Contratación Pública	Operador		D2-06	38	PASA
10.10.11.43	Departamento de Contratación Pública	Administrativo		D2-13	1	FALLA
10.10.11.45	Dirección de Logística	Administrativo		D2-05	3	PASA
10.10.11.52	Dirección de Sanidad	Director		D1-06	6	PASA
10.10.11.53	Dirección de Sanidad	Subdirector		D1-02	2	PASA
10.10.11.54	Dirección de Sanidad	Secretaría		D1-08	8	PASA
10.10.11.55	Dirección de Sanidad	Digitador		D1-07	7	PASA
10.10.11.56	Dirección de Sanidad	Administrativo	Jack dañado	D1-09	9	PASA
10.10.11.57	Dirección de Sanidad	Jefatura		D1-12	12	PASA
10.10.11.58	Dirección de Sanidad	Medicina Preventiva		D1-10	10	PASA
10.10.11.59	Dirección de Sanidad	Dpto. Estadística	Jack dañado	D1-11	11	PASA

10.10.11.60	Dirección de Sanidad	Asistente Planificación		D1-19	19	PASA
10.10.11.61	Dirección de Sanidad	Jefatura		D1-16	16	PASA
10.10.11.62	Dirección de Sanidad	Planificación		D1-14	14	PASA
10.10.11.63	Dirección de Sanidad	Estadísticas		D1-13	13	PASA
10.10.11.64	Dirección de Sanidad	Libre/Sala de Sesiones		D1-01	.	PASA
10.10.11.65	Dirección de Sanidad	Libre	Jack dañado	D1-03	.	PASA
10.10.11.66	Dirección de Sanidad	Libre		D1-46	.	FALLA

BLOQUE 4						
IP:	**10.10.12.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.12.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.12.9	Dirección de Telecomunicaciones	Asesoría jurídica		D2-03	29(2)	PASA
10.10.12.10	Dirección de Telecomunicaciones	Director		D1-43	43(1)	PASA
10.10.12.11	Dirección de Telecomunicaciones	Secretaría	Sin Etiqueta	D1-46	46(1)	PASA
10.10.12.12	Dirección de Telecomunicaciones	Dpto. Control y Evaluación		V1-44	16(2)	PASA
10.10.12.13	Dirección de Telecomunicaciones	Administrativo		D1-37	37(1)	PASA
10.10.12.14	Dirección de Telecomunicaciones	Administrativo	Jack Flojo	D1-39	39(1)	PASA
10.10.12.15	Dirección de Telecomunicaciones	Administrativo		D1-41	41(1)	FALLA
10.10.12.16	Dirección de Telecomunicaciones	Libre		D1-36	36(1)	PASA
10.10.12.17	Dirección de Telecomunicaciones Logística	Jefatura		D1-38	38(1)	PASA

10.10.12.18	Dirección de Telecomunicaciones Logística	Activos Fijos		D1-35	17(1)	FALLA
10.10.12.19	Dirección de Telecomunicaciones Logística	Administrativo		D1-34	34(1)	PASA
10.10.12.20	Dirección de Telecomunicaciones Logística	Presupuesto		D1-33	9(1)	PASA
10.10.12.23	Dirección de Sistemas	Director		D1-44	.	PASA
10.10.12.25	Dirección de Telecomunicaciones	Administrativo		D1-40	40(1)	FALLA
10.10.12.26	Dirección de Telecomunicaciones	Jefatura		D1-28	28(1)	PASA
10.10.12.28	Dirección de Telecomunicaciones	Administrativo		D1-27	27(1)	PASA
10.10.12.30	Dirección de Telecomunicaciones	Administrativo		D1-29	29(1)	PASA
10.10.12.31	Dirección de Telecomunicaciones	Secretaría		D1-30	30(1)	PASA
10.10.12.33	Dirección de Telecomunicaciones	Jefatura		D1-25	25(1)	PASA
10.10.12.34	Dirección de Telecomunicaciones	Administrativo		D1-31	31(1)	PASA
10.10.12.36	Dirección de Telecomunicaciones	Administrativo		D1-32	32(1)	PASA
10.10.12.48	Dirección de Sistemas	Amanuense		D1-45	45(1)	PASA
10.10.12.49	Dirección de Sistemas	Jefatura		D2-11	7(2)	PASA
10.10.12.50	Dirección de Sistemas	Secretaría		D2-10	9(2)	PASA
10.10.12.51	Dirección de Sistemas	Supervisor	puente a V2-17 para conectarse al core	D2-08	3	FALLA
10.10.12.52	Dirección de Sistemas	Supervisor		D2-25	35(2)	PASA
10.10.12.53	Dirección de Sistemas	Planificador		D2-07	5(2)	PASA
10.10.12.54	Dirección de Sistemas	Suministros		D2-13	37(2)	PASA
10.10.12.56	Dirección de Sistemas	Sala de Reuniones		D2-09	12(2)	PASA
10.10.12.60	Dirección de Sistemas	Técnico Soporte	Conexión con el SW INF 8 puertos	D2-05	4(2)	PASA
10.10.12.67	Dirección de Sistemas	Técnico Soporte		D2-06	22(2)	FALLA
10.10.12.74	Dirección de Sistemas	Técnico Soporte	Sin Etiqueta	D2-17	.	PASA

10.10.12.75	Dirección de Sistemas	Desarrollador		D2-26	6(2)	PASA
10.10.12.76	Dirección de Sistemas	Administrativo		D2-27	2(2)	PASA
10.10.12.77	Dirección de Sistemas	Administrativo		D2-28	11(2)	PASA
10.10.12.78	Dirección de Sistemas	Supervisor		D2-29	28(2)	PASA
10.10.12.79	Dirección de Sistemas	Planificador		D2-30	3(2)	FALLA
10.10.12.80	Dirección de Sistemas	Planificador		D2-31	38(2)	PASA
10.10.12.81	Dirección de Sistemas	Amanuense		D2-32	14(2)	PASA
10.10.12.82	Dirección de Telecomunicaciones	Planificador		V1-33	26(2)	PASA
10.10.12.83	Dirección Administrativa-Finanzas	Planificador		V1-11	25(2)	PASA
10.10.12.84	Dirección de Sistemas	Director	cable directo	D2-20	31(2)	PASA
10.10.12.85	Dirección de Sistemas	Libre		V2-17	23(2)	PASA
10.10.12.86	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.87	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.88	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.89	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.90	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.91	Dirección de Sistemas	Técnico Soporte		Alim sw inf	.	SIN CERT
10.10.12.92	Dirección de Sistemas	Supervisor		D2-21	33(2)	PASA
10.10.12.93	Dirección de Sistemas	Desarrollador		D2-22	32(2)	PASA
10.10.12.94	Dirección de Sistemas	Desarrollador		D2-23	34(2)	PASA
10.10.12.95	Dirección de Sistemas	Desarrollador		D2-24	10(2)	PASA
10.10.12.96	Dirección de Sistemas	Técnico Soporte		D2-04		PASA
10.10.12.97	Dirección de Sistemas	Administrativo		D1-26	26(1)	PASA
10.10.12.98	Dirección de Sistemas	Técnico Soporte		V2-12	40(2)	PASA
10.10.12.99	Dirección Administrativa-Finanzas	Subdirector		D1-01	1(1)	PASA
10.10.12.100	Dirección Administrativa-Finanzas	Secretaría		D1-06	6(1)	PASA
10.10.12.101	Dirección Administrativa-Finanzas	Contabilidad		D1-04	4(1)	PASA
10.10.12.102	Dirección Administrativa-Finanzas	Contabilidad		D1-08	8(1)	PASA

10.10.12.103	Dirección Administrativa-Finanzas	Contabilidad		D1-09	12(1)	PASA
10.10.12.104	Dirección Administrativa-Finanzas	Contabilidad		D1-10	10(1)	PASA
10.10.12.105	Dirección de Telecomunicaciones	Jefatura		D1-21	21(1)	PASA
10.10.12.106	Dirección Administrativa-Finanzas	Presupuesto		D1-20	20(1)	PASA
10.10.12.107	Dirección Administrativa-Finanzas	Presupuesto		D1-15	15(1)	PASA
10.10.12.108	Dirección Administrativa-Finanzas	Presupuesto	Sin Face Plate	D1-14	14(1)	PASA
10.10.12.109	Dirección Administrativa-Finanzas	Activos Fijos		D1-16	16(1)	PASA
10.10.12.110	Dirección Administrativa-Finanzas	Subjefatura		D1-02	2(1)	PASA
10.10.12.111	Dirección Administrativa-Finanzas	Presupuesto		D1-11	11(1)	PASA
10.10.12.112	Dirección Administrativa-Finanzas	Presupuesto		D1-12	13(2)	PASA
10.10.12.113	Dirección Administrativa-Finanzas	Administrativo		D1-05	5(1)	PASA
10.10.12.114	Dirección Administrativa-Finanzas	Administrativo		D1-18	18(2)	PASA
10.10.12.115	Dirección Administrativa-Finanzas	Activos Fijos		D1-19	19(1)	PASA
10.10.12.116	Comité de Contrataciones	Amanuense		D2-01	.	PASA
10.10.12.117	Comité de Contrataciones	Jefatura		D2-02	1(2)	PASA
10.10.12.118	Dirección Administrativa-Finanzas	Administrativo		V1-05	.	PASA
	Departamento de Control y Evaluación	Libre		D2-16	.	PASA
	Departamento de Control y Evaluación	Libre	Jack Suelto	D2-14	.	FALLA
	Dirección Administrativa-Finanzas	Libre		D1-07	.	PASA

	Dirección Administrativa-Finanzas	Libre	Jack Suelto - Sin etiqueta	D1-13	.	PASA
10.10.12.119	Dirección Administrativa-Finanzas	Administrativo		D1-17	18(1)	PASA
	Dirección Administrativa-Finanzas	Libre/Archivo		D1-24	.	PASA
	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-48	.	PASA
	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-47	.	PASA
	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-42	.	PASA

BLOQUE 5						
IP:	**10.10.13.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.13.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.13.10	Jefatura	Jefatura	Sin etiqueta	D1-18	18	PASA
10.10.13.11	Jefatura	Oficial Ayudante		D1-23	23	PASA
10.10.13.12	Jefatura	Secretaría		D1-21	21	PASA
10.10.13.13	Jefatura	Amanuense		D1-20	20	PASA
10.10.13.14	Secretaría General	Jefatura		D1-14	14	PASA
10.10.13.15	Asesoría Especializada	Asesoría Especializada		D1-10	10	FALLA
10.10.13.16	Secretaría General	Libre		D1-06	.	PASA
10.10.13.17	Secretaría General	Administrativo		D1-13	13	PASA
10.10.13.18	Secretaría General	Administrativo		D1-11	12	PASA
10.10.13.19	Secretaría General	Administrativo		D1-12	8	PASA
10.10.13.24	Jefatura Estado Mayor	Jefatura		D1-28	28	PASA
10.10.13.25	Jefatura Estado Mayor	Oficial Ayudante		D1-25	25	PASA
10.10.13.26	Jefatura Estado Mayor	Secretaría		V1-38	39	FALLA

10.10.13.27	Jefatura Estado Mayor	Amanuense		D1-30	30	FALLA
10.10.13.28	Intereses Nacionales	Jefatura		D1-01	1	PASA
10.10.13.29	Intereses Nacionales	Secretaría		D1-02	2	PASA
10.10.13.30	Intereses Nacionales	Administrativo		D1-03	3	PASA
10.10.13.31	Intereses Nacionales	Asesoría Especializada		D1-05	5	PASA
10.10.13.32	Asesoría Jurídica	Amanuense		D1-09	9	PASA
10.10.13.33	Asesoría Jurídica	Amanuense		D1-07	4	PASA
10.10.13.38	Dirección de Desarrollo Institucional	Jefatura		D1-35	35	PASA
10.10.13.39	Dirección de Desarrollo Institucional	Secretaría		D1-36	36	FALLA
10.10.13.40	Dirección de Desarrollo Institucional	Asesoría Naval		D1-38	38	FALLA
10.10.13.41	Dirección de Desarrollo Institucional	Amanuense		D1-42	42	PASA
10.10.13.42	Dirección de Desarrollo Institucional	Asesor civil		D1-41	41	PASA
10.10.13.43	Dirección de Desarrollo Institucional	Sala de Reuniones		D1-43	43	PASA
10.10.13.45	Dirección de Desarrollo Institucional	Asesor Aéreo		D1-33	33	PASA
10.10.13.46	Dirección de Desarrollo Institucional	Amanuense		D1-31	31	PASA
10.10.13.47	Dirección de Desarrollo Institucional	Administrativo		D1-40	7	PASA
10.10.13.53	Dirección de Planificación POA	Analista financiero		D1-48	48	PASA
10.10.13.50	Asesoría Especializada	Asesoría Especializada		V2-19	37	PASA
10.10.13.51	Dirección de Desarrollo Institucional	Administrativo		V2-20	44	PASA
10.10.13.52	Dirección de Desarrollo Institucional	Administrativo		D1-34	34	PASA
	Intereses Nacionales	Libre/Comité Asesor		D1-04	.	PASA
	Asesoría Jurídica	Libre	Sin etiqueta	D1-08	.	PASA
	Asesoría Jurídica	Libre		D1-19	.	PASA
	Sala de Reuniones	Libre		D1-15	.	PASA

	Sala de Reuniones	Libre		D1-24	.	PASA
	Sala de Reuniones	Libre		D1-16	.	PASA
	Jefatura Estado Mayor	Libre		D1-26	.	PASA
	Jefatura Estado Mayor	Libre		D1-27	.	PASA
	Jefatura Estado Mayor	Libre		D1-29	.	PASA
	Dirección de Desarrollo Institucional	Libre		D1-39	.	PASA
	Dirección de Desarrollo Institucional	Libre/Sala de Reuniones		D1-45	.	PASA
	Dirección de Desarrollo Institucional	Libre/Sala de Reuniones		D1-46	.	PASA
	Dirección de Desarrollo Institucional	Libre		D1-47	.	PASA
10.10.13.58	Jefatura	Sala de Reuniones	Sin etiqueta	V1-22	22	PASA
	Sala de Estado Mayor	Libre	Sin etiqueta	V1-20	.	PASA
10.10.13.55	Dirección de Desarrollo Institucional	Administrativo	Sin etiqueta	V2-17	26	PASA
	Departamento de Seguridad	Libre	Sin etiqueta	DIRECTO	.	PASA
	Departamento de Seguridad	Libre	Sin etiqueta	DIRECTO	.	FALLA
10.10.13.59	Dirección de Desarrollo Institucional	Administrativo		D1-32	32	PASA
10.10.13.60	Dirección de Planificación	Administrativo		V2-18	16	PASA

BLOQUE 6

IP:	**10.10.14.x**
Mascara:	**255.255.255.0**
Gateway:	**10.10.14.254**

DIRECCIÓN IP	DEPENDENCIA	CARGO-USUARIO	OBSERVACIONES	TOMA	PORT.	CERTIFICACIÓN
10.10.14.10	Dirección de Operaciones	Dirección		D1-28	46	FALLA
10.10.14.11	Dirección de Operaciones	Subdirector		D1-29	44	PASA
10.10.14.12	Dirección de Operaciones	Secretaria		D1-31	11	PASA
10.10.14.13	Dirección de Operaciones	Administrativo		D1-37	19	PASA
10.10.14.14	Dirección de Desarrollo	Director		D1-34	15	PASA
10.10.14.15	Dirección de Desarrollo	Secretaria		D1-35	17	PASA

10.10.14.16	Dirección de Operaciones	Planificación		D2-02	2	PASA
10.10.14.21	Dirección de Cooperación Interinstitucional	Jefatura		D1-06	5	PASA
10.10.14.22	Dirección de Cooperación Interinstitucional	Coordinación		CD	3	PASA
10.10.14.24	Dirección de Cooperación Interinstitucional	Misiones de Paz		D1-07	40	PASA
10.10.14.25	Dirección de Cooperación Interinstitucional	Secretaria	Switch 8 Puertos TrendNet	D2-21	12	PASA
10.10.14.26	Dirección de Cooperación Interinstitucional	Amanuense	Cajetín dañado	D1-09	39	PASA
10.10.14.27	Dirección de Cooperación Interinstitucional	Misiones de Paz		V1-10	32	FALLA
10.10.14.32	Dirección de Doctrina Conjunta y Educación	Jefatura		D1-10	33	PASA
10.10.14.33	Dirección de Doctrina Conjunta y Educación	Secretaria	Sin etiqueta	D1-15	25	FALLA
10.10.14.34	Dirección de Doctrina Conjunta y Educación	Administrativo		D2-04	47	PASA
10.10.14.36	Dirección de Doctrina Conjunta y Educación	Administrativo	Sin etiqueta	D2-19	11	PASA
10.10.14.38	Dirección de Doctrina Conjunta y Educación	Coordinación		D2-20	14	PASA
10.10.14.40	Departamento de Control y Evaluación	Jefatura		D1-22	41	PASA
10.10.14.42	Centro de Coordinación Petrolera	Planificación		V1-13	30	FALLA
10.10.14.43	Centro de Coordinación Petrolera	Administrativo		D2-06	9	PASA
10.10.14.45	Departamento de Planes y Ordenes	Subjefatura		D1-11	42	PASA
10.10.14.46	Departamento de Planes y Ordenes	Administrativo		D2-08	10	PASA
10.10.14.47	Departamento de Planes y Ordenes	Administrativo		D2-13	28	PASA
10.10.14.48	Departamento de Planes y Ordenes	Administrativo		D2-14	27	PASA
10.10.14.49	Departamento de Planes y	Asesor		D2-16	26	PASA

	Ordenes					
10.10.14.51	Departamento Militar	Amanuense		D1-08	37	PASA
10.10.14.52	Departamento de Planes y Ordenes	Amanuense		D1-20	.	PASA
	Departamento de Planes y Ordenes	Libre		D1-17	.	PASA
10.10.14.57	Federación deportiva	Jefatura		D1-01	1	PASA
10.10.14.58	Federación deportiva	Administrativo		D1-02	6	FALLA
10.10.14.59	Federación deportiva	Administrativo		D1-04	4	PASA
10.10.14.60	Federación deportiva	Administrativo		D1-03	7	FALLA
10.10.14.62	Federación deportiva	Amanuense		D2-22	16	PASA
10.10.14.63	Federación deportiva	Administrativo		D1-14	38	FALLA
10.10.14.67	Departamento de Comunicación Social	Jefatura		D1-40	18	PASA
10.10.14.69	Departamento de Comunicación Social	Administrativo		D1-42	20	PASA
10.10.14.72	Departamento de Comunicación Social	Inst AP Wireless		D1-41	24	PASA
	Departamento de Comunicación Social	Supervisor		D1-43	.	PASA
	Departamento de Planes y Ordenes	Libre		V2-03	.	PASA
10.10.14.75	Departamento de Planes y Ordenes	Jefatura		D1-39	21	PASA
10.10.14.76	Departamento de Planes y Ordenes	Amanuense		V1-40	31	PASA
10.10.14.77	Departamento de Planes y Ordenes	Planificación		D1-38	8	PASA
10.10.14.78	Departamento de Planes y Ordenes	Control		D1-36	13	PASA
	Departamento de Control y Evaluación	Libre		D1-27	.	PASA
	Departamento Administrativo	Libre		D1-32	.	PASA
	Departamento de Planes y Ordenes	Libre		D2-07	.	PASA
	Departamento de Planes y	Libre		D2-03	VOZ	PASA

	Ordenes					
	Departamento de Control y Evaluación	Libre		D2-05	.	PASA
	Departamento de Control y Evaluación	Libre	Sin etiqueta	D1-21	.	PASA
	Sala de Reuniones	Libre		D1-26	.	PASA
10.10.14.80	Dirección de Operaciones	Sala de Reuniones		D1-23	45	PASA
10.10.14.81	Dirección de Operaciones	Sala de Reuniones		D1-24	.	PASA
10.10.14.82	Dirección de Operaciones	Administrativo		D1-12	36	PASA
10.10.14.83	Dirección de Operaciones	Administrativo		D1-19	34	PASA
	Dirección de Operaciones	Libre		D2-15	.	PASA

BLOQUE 7						
IP:	**10.10.15.x**					
Mascara:	**255.255.255.0**					
Gateway:	**10.10.15.254**					
DIRECCIÓN IP	**DEPENDENCIA**	**CARGO-USUARIO**	**OBSERVACIONES**	**TOMA**	**PORT.**	**CERTIFICACIÓN**
10.10.15.21	Dirección de Investigación	Administrativo		D2-15	**1**	PASA
10.10.15.10	Dirección de Investigación	Administrativo		D2-10	2	PASA
10.10.15.11	Dirección de Investigación	Técnico Soporte		D2-30	5	PASA
10.10.15.12	Dirección de Investigación	Administrativo		D2-19	6	PASA
10.10.15.13	Dirección de Investigación	Suministros		D2-21	7	PASA
10.10.15.14	Dirección de Investigación	Administrativo		D2-31	8	PASA
10.10.15.15	Dirección de Investigación	Técnico Soporte		D2-17	9	PASA
10.10.15.16	Dirección de Investigación	Administrativo		D2-20	10	PASA
10.10.15.17	Dirección de Investigación	Planificación		D2-42	11	PASA
10.10.15.18	Dirección de Investigación	Planificación		D2-23	12	PASA
10.10.15.19	Dirección de Investigación	Supervisor		D1-32	14	PASA
10.10.15.20	Dirección de Investigación	Administrativo		D2-07	15	PASA
	Dirección de Investigación	Libre		D2-03		FALLA
10.10.15.22	Dirección de Investigación	Planificación		D2-05	17	PASA
10.10.15.23	Dirección de Investigación	Planificación		D2-24	18	PASA
10.10.15.24	Dirección de Investigación	Planificación		D1-26	19	PASA
10.10.15.25	Dirección de Investigación	Planificación		D1-23	20	PASA

ANEXO 2. DISPONIBILIDAD DEL EQUIPAMIENTO ACTIVO

SW BLOQUE 1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

	PUERTOS OCUPADOS	18
	PUERTOS LIBRES	6

SW 1 - BLOQUE 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

	PUERTOS OCUPADOS	36
	PUERTOS LIBRES	12

SW 2 - BLOQUE 2

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

	PUERTOS OCUPADOS	15
	PUERTOS LIBRES	33

SW 3 - BLOQUE 2

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

PUERTOS OCUPADOS	12
PUERTOS LIBRES	4

SW BLOQUE 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

PUERTOS OCUPADOS	43
PUERTOS LIBRES	5

SW 1 - BLOQUE 4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

PUERTOS OCUPADOS	36
PUERTOS LIBRES	12

SW 2 - BLOQUE 4

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

PUERTOS OCUPADOS	29
PUERTOS LIBRES	19

SW BLOQUE 5

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

PUERTOS OCUPADOS	37
PUERTOS LIBRES	11

SW BLOQUE 6

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

PUERTOS OCUPADOS	42
PUERTOS LIBRES	6

SW BLOQUE 7

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

PUERTOS OCUPADOS	16
PUERTOS LIBRES	8

ANEXO 3. PRUEBAS DE CERTIFICACIÓN

Las pruebas de cableado estructurado fueron realizadas a 373 puntos de red, dentro de los cuales como se indica en el capítulo 2, 342 puntos pasaron las pruebas de certificación mientras que 31 puntos no lo hicieron. En este anexo se indica una muestra correspondiente a 10 pruebas de certificación tomadas indistintamente, de las cuales 5 puntos están relacionados al cumplimiento de todos los parámetros mínimos de certificación y 5 pruebas relacionadas al incumplimiento de las mismas; de éstas últimas, 3 puntos con errores en el mapa de cableado y 2 con problemas internos. Las pruebas de certificación totales se anexan en el CD adjunto.

De los 3 puntos que no pasaron las pruebas de certificación debido a problemas en el mapa de cableado se evidencia que dos de los puntos tienen problemas en el jack del extremo principal del certificador, dado que la distancia que se muestra pertenece a la longitud del enlace de comprobación, mientras que uno de ellos tiene problemas en el extremo remoto. De la verificación de las pruebas realizadas se puede determinar que en los casos mencionados es necesario una reinstalación de los jack, con lo cual se habiliten dichos puntos y se cumpla con las pruebas de certificación realizadas.

De los 2 puntos de red adicionales que no cumplieron los parámetros de certificación tuvieron problemas ocasionados a problemas internos en el cable con valores más altos de la media permitida.

Dentro de los principales problemas relacionados a dichos puntos de red es conveniente tener en cuenta la distancia del enlace la misma que no debe sobrepasar la distancia establecida igual a 90 metros, además valores relacionados a la resistencia del cableado pueden verse afectados por el tiempo del uso del mismo, o debido al medio al cual se encuentran expuestos.

Además el uso de buenas prácticas a al hora de realizar el cableado es de vital importancia tanto para el paso del cableado como el ponchado de los mismos, debido que la tención excesiva y/o el destrenzado del cable lo cual influye en la

transmisión. Así mismo es recomendable que se revise el estado de los conectores en los dos extremos.

Es importante tener en cuenta que de las pruebas realizadas debe evaluarse la factibilidad de habilitación de los puntos en función del problema asociado y de no ser posible su solución deshabilitarlos permanentemente dado que no se puede asegurar su conexión.

La muestra de las pruebas de certificación tomadas como ejemplo se indican a continuación:

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID: D2-26

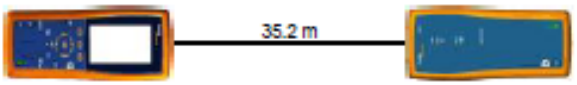
Test Summary: PASS

Date / Time: 01/21/2010 09:37:12am
Headroom: 6.1 dB (NEXT 12-36)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

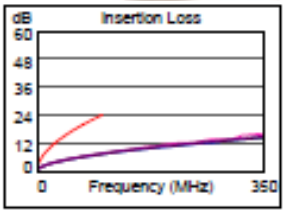
Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

Model: DTX-1800
Main S/N: 9859001
Remote S/N: 9859002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

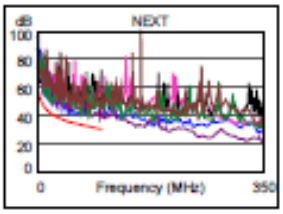
Wire Map (T568B)
PASS

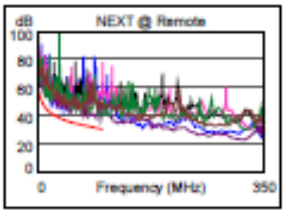


Length (m), Limit 100.0	[Pair 12]	35.2
Prop. Delay (ns), Limit 555		175
Delay Skew (ns), Limit 50		5
Resistance (ohms)	[Pair 12]	6.4
Insertion Loss Margin (dB)	[Pair 78]	16.5
Frequency (MHz)	[Pair 78]	100.0
Limit (dB)	[Pair 78]	24.0

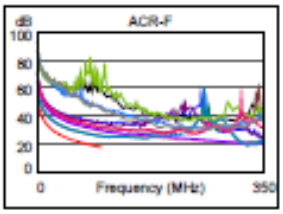


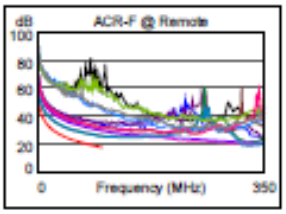
	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	12-36	36-45	36-45	36-45
NEXT (dB)	6.1	6.9	6.4	6.9
Freq. (MHz)	59.8	97.5	84.3	97.8
Limit (dB)	33.9	30.3	31.4	30.2
Worst Pair	36	36	45	36
PS NEXT (dB)	6.6	7.4	8.6	8.0
Freq. (MHz)	23.5	30.1	84.3	97.8
Limit (dB)	37.8	36.0	28.4	27.2



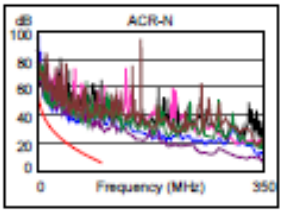


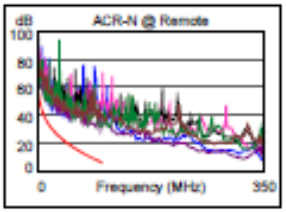
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	45-36	45-36
ACR-F (dB)	6.0	6.0	7.6	7.8
Freq. (MHz)	2.0	1.6	95.0	98.3
Limit (dB)	51.4	53.2	17.8	17.6
Worst Pair	36	36	36	36
PS ACR-F (dB)	7.7	7.7	9.6	9.5
Freq. (MHz)	1.0	1.6	99.0	99.0
Limit (dB)	54.4	50.2	14.5	14.5



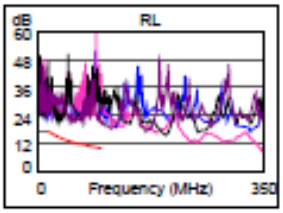


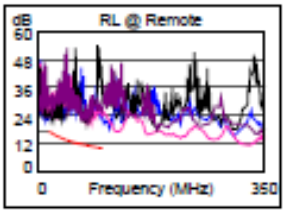
N/A	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	36-45
ACR-N (dB)	12.1	12.4	24.5	23.5
Freq. (MHz)	2.5	2.9	97.5	97.8
Limit (dB)	53.4	52.1	6.6	6.5
Worst Pair	36	36	45	36
PS ACR-N (dB)	13.4	14.2	26.7	24.4
Freq. (MHz)	1.6	1.8	97.5	97.8
Limit (dB)	53.9	53.4	3.6	3.5





PASS	MAIN	SR	MAIN	SR
Worst Pair	12	12	78	36
RL (dB)	5.7	5.1	10.4	9.3
Freq. (MHz)	21.9	22.0	100.0	82.8
Limit (dB)	16.6	16.6	10.0	10.8





Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-18 Active	TR-18 Passive	

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID: D2-20

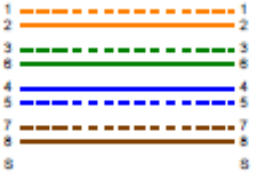
Test Summary: PASS

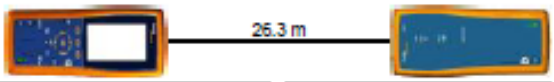
Date / Time: 01/21/2010 09:29:41am
Headroom: 5.0 dB (NEXT 36-45)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

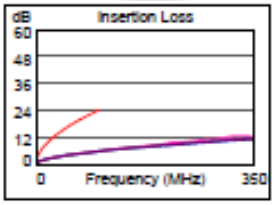
Model: DTX-1600
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
PASS

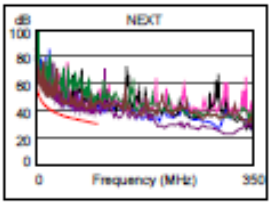


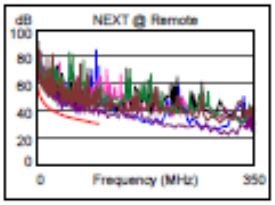


Length (m), Limit 100.0	[Pair 12]	26.3
Prop. Delay (ns), Limit 555		130
Delay Skew (ns), Limit 50		3
Resistance (ohms)	[Pair 12]	5.1
Insertion Loss Margin (dB)	[Pair 36]	18.2
Frequency (MHz)	[Pair 36]	100.0
Limit (dB)	[Pair 36]	24.0

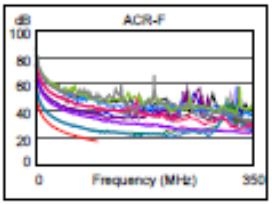


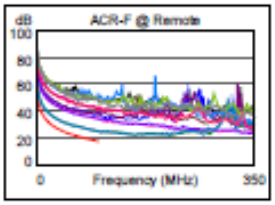
	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	36-45
NEXT (dB)	5.7	5.0	6.0	6.5
Freq. (MHz)	41.3	41.0	91.0	90.8
Limit (dB)	36.7	36.7	30.8	30.8
Worst Pair	36	36	45	45
PS NEXT (dB)	7.0	6.4	7.4	8.5
Freq. (MHz)	41.3	41.3	91.0	90.8
Limit (dB)	33.7	33.7	27.8	27.8



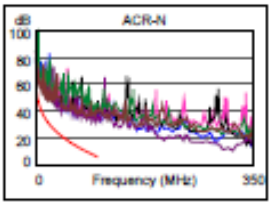


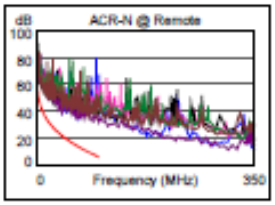
PASS	MAIN	SR	MAIN	SR
Worst Pair	45-36	36-45	45-36	36-45
ACR-F (dB)	5.3	5.2	7.0	7.2
Freq. (MHz)	1.0	1.0	99.5	99.3
Limit (dB)	57.4	57.4	17.4	17.5
Worst Pair	36	45	36	45
PS ACR-F (dB)	7.9	7.8	9.7	9.6
Freq. (MHz)	1.0	1.0	99.5	99.5
Limit (dB)	54.4	54.4	14.4	14.4



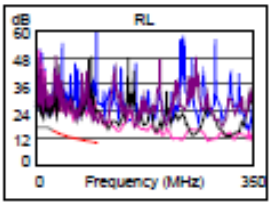


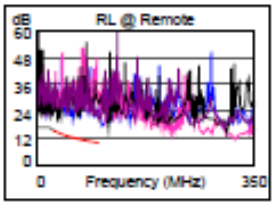
N/A	MAIN	SR	MAIN	SR
Worst Pair	45-78	45-78	36-45	36-45
ACR-N (dB)	13.4	14.4	25.2	24.0
Freq. (MHz)	6.4	2.0	100.0	90.8
Limit (dB)	44.6	55.3	6.1	8.0
Worst Pair	45	78	36	45
PS ACR-N (dB)	14.6	15.5	26.6	26.0
Freq. (MHz)	3.3	5.9	100.0	90.8
Limit (dB)	48.0	42.4	3.1	5.0





PASS	MAIN	SR	MAIN	SR
Worst Pair	45	45	78	45
RL (dB)	6.8	5.1	8.9	5.1
Freq. (MHz)	34.8	34.8	99.8	34.8
Limit (dB)	14.6	14.6	10.0	14.6





Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID: D2-14

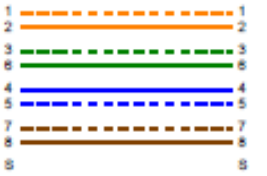
Test Summary: PASS

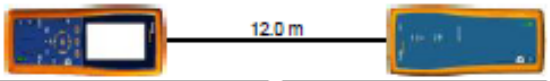
Date / Time: 01/27/2010 12:40:01pm
Headroom: 6.3 dB (NEXT 12-36)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

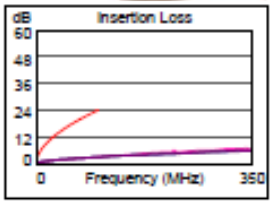
Model: DTX-1600
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
PASS

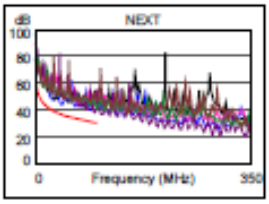


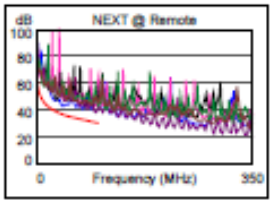


Length (m), Limit 100.0	[Pair 78]	12.0
Prop. Delay (ns), Limit 555		59
Delay Skew (ns), Limit 50		1
Resistance (ohms)	[Pair 12]	2.8
Insertion Loss Margin (dB)	[Pair 36]	21.1
Frequency (MHz)	[Pair 36]	100.0
Limit (dB)	[Pair 36]	24.0

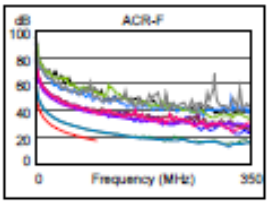


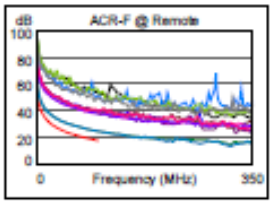
	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	36-45	36-45
NEXT (dB)	7.4	6.3	7.6	7.6
Freq. (MHz)	42.8	42.3	96.3	95.5
Limit (dB)	36.4	36.5	30.4	30.4
Worst Pair	12	12	36	45
PS NEXT (dB)	8.7	7.8	9.6	9.1
Freq. (MHz)	42.8	42.8	97.0	95.5
Limit (dB)	33.4	33.4	27.3	27.4



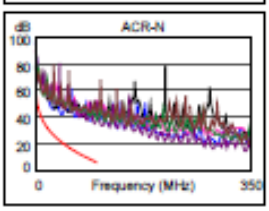


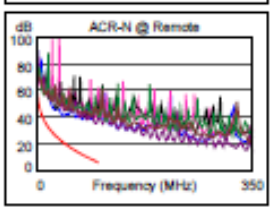
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	45-36
ACR-F (dB)	6.1	6.0	6.8	6.8
Freq. (MHz)	1.1	1.1	100.0	100.0
Limit (dB)	56.4	56.4	17.4	17.4
Worst Pair	36	36	36	36
PS ACR-F (dB)	8.9	8.9	9.6	9.6
Freq. (MHz)	1.1	1.1	99.5	100.0
Limit (dB)	53.4	53.4	14.4	14.4



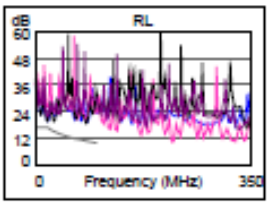


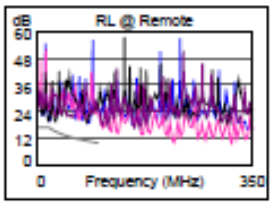
N/A	MAIN	SR	MAIN	SR
Worst Pair	45-78	45-78	36-45	36-45
ACR-N (dB)	15.7	16.1	28.4	28.2
Freq. (MHz)	1.6	1.6	96.3	95.5
Limit (dB)	56.9	56.9	6.8	7.0
Worst Pair	78	78	36	45
PS ACR-N (dB)	15.0	15.5	30.3	29.7
Freq. (MHz)	1.6	1.6	97.0	95.5
Limit (dB)	53.9	53.9	3.7	4.0





N/A	MAIN	SR	MAIN	SR
Worst Pair	45	12	45	12
RL (dB)	2.7	2.9	8.0	8.2
Freq. (MHz)	19.6	20.5	82.8	84.5
Limit (dB)	17.0	16.9	10.8	10.7





Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID: D1-47

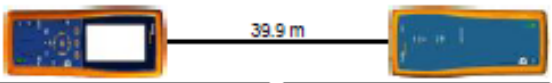
Test Summary: PASS

Date / Time: 01/20/2010 03:02:51pm
Headroom: 3.3 dB (NEXT 36-45)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

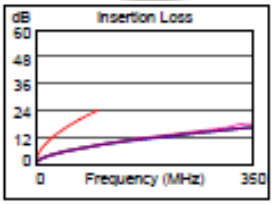
Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

Model: DTX-1800
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

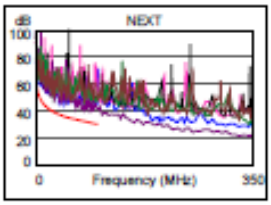
Wire Map (T568B)
PASS

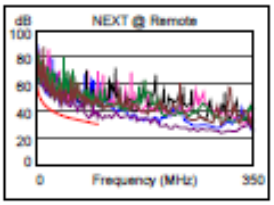


Length (m), Limit 100.0	[Pair 12]	39.9
Prop. Delay (ns), Limit 555		198
Delay Skew (ns), Limit 50		5
Resistance (ohms)	[Pair 12]	7.3
Insertion Loss Margin (dB)	[Pair 36]	15.6
Frequency (MHz)	[Pair 36]	100.0
Limit (dB)	[Pair 36]	24.0

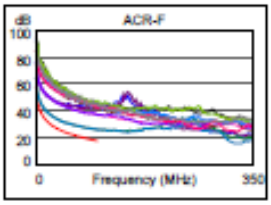


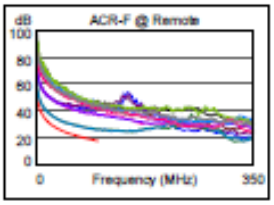
	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	36-45
NEXT (dB)	7.7	3.3	7.7	3.4
Freq. (MHz)	87.8	84.3	87.8	87.5
Limit (dB)	31.1	31.4	31.1	31.1
Worst Pair	36	45	36	45
PS NEXT (dB)	9.4	5.8	9.4	5.8
Freq. (MHz)	87.8	87.3	87.8	87.3
Limit (dB)	28.1	28.1	28.1	28.1



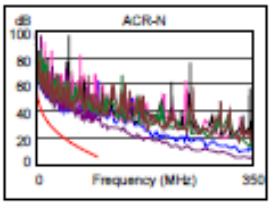


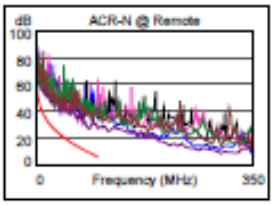
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	45-36
ACR-F (dB)	6.1	6.1	8.0	7.8
Freq. (MHz)	1.4	3.8	98.0	98.3
Limit (dB)	54.6	45.9	17.6	17.6
Worst Pair	36	45	45	45
PS ACR-F (dB)	8.9	8.8	10.7	10.8
Freq. (MHz)	1.3	3.8	98.0	100.0
Limit (dB)	52.5	42.9	14.6	14.4



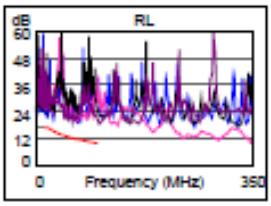


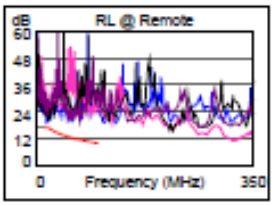
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	36-45	36-45
ACR-N (dB)	14.1	13.9	24.4	18.0
Freq. (MHz)	7.1	7.4	99.0	87.5
Limit (dB)	43.5	43.1	6.3	8.8
Worst Pair	12	12	36	36
PS ACR-N (dB)	15.1	14.6	25.8	22.6
Freq. (MHz)	6.9	6.9	99.0	98.8
Limit (dB)	40.8	40.8	3.3	3.3





PASS	MAIN	SR	MAIN	SR
Worst Pair	12	12	12	12
RL (dB)	3.6	2.5	7.3	2.5
Freq. (MHz)	19.3	19.3	68.8	19.3
Limit (dB)	17.0	17.0	11.6	17.0





Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: D1-46

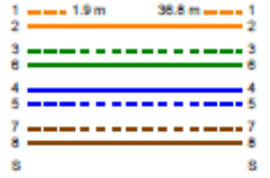
Test Summary: FAIL

Date / Time: 01/24/2010 10:58:30am
Headroom: -1.6 dB (NEXT 12-36)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

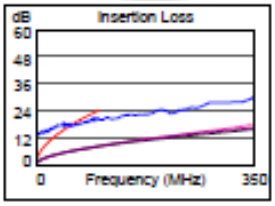
Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

Model: DTX-1800
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

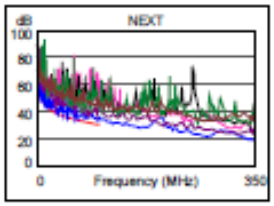
Wire Map (T568B)
FAIL

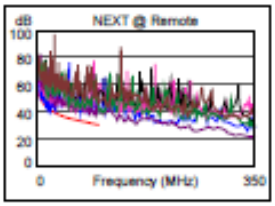


Length (m), Limit 100.0	[Pair 12]	1.9
Prop. Delay (ns), Limit 555		193
Delay Skew (ns), Limit 50		184 F
Resistance (ohms)	[Pair 12]	Open
Insertion Loss Margin (dB)	[Pair 12]	-10.3 F
Frequency (MHz)	[Pair 12]	1.9
Limit (dB)	[Pair 12]	3.0

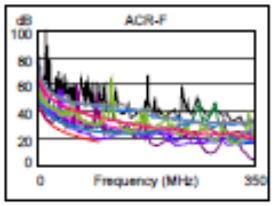


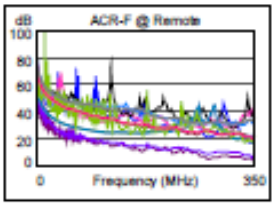
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	12-36	36-45
NEXT (dB)	-1.6 F	-0.5 F	2.7	6.9
Freq. (MHz)	2.9	20.9	98.8	93.5
Limit (dB)	55.9	41.7	30.2	30.6
Worst Pair	36	12	36	36
PS NEXT (dB)	1.0	2.0	3.8	8.7
Freq. (MHz)	2.9	20.9	81.5	97.0
Limit (dB)	52.9	38.7	28.6	27.3



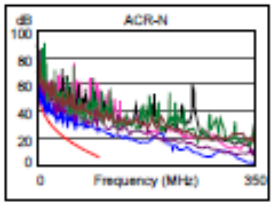


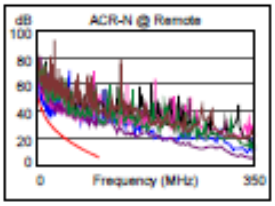
FAIL	MAIN	SR	MAIN	SR
Worst Pair	36-12	36-12	45-12	36-12
ACR-F (dB)	0.3*	-7.7 F	1.8	-2.5
Freq. (MHz)	16.1	5.8	98.5	98.5
Limit (dB)	33.3	42.2	17.5	17.5
Worst Pair	12	36	12	45
PS ACR-F (dB)	2.1	2.2	4.4	3.8
Freq. (MHz)	16.1	1.0	98.5	98.5
Limit (dB)	30.3	54.4	14.5	14.5



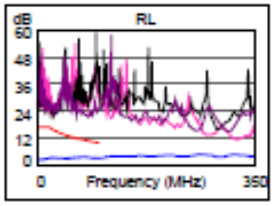


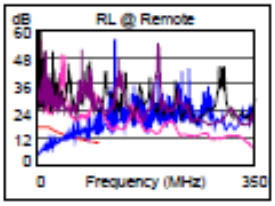
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	12-36	36-45
ACR-N (dB)	0.9	5.9	18.6	22.5
Freq. (MHz)	2.9	11.9	98.8	93.5
Limit (dB)	52.1	38.0	6.3	7.4
Worst Pair	12	12	12	12
PS ACR-N (dB)	-8.1	-3.6	8.0	16.0
Freq. (MHz)	2.9	12.0	99.0	100.0
Limit (dB)	49.1	34.9	3.3	3.1





FAIL	MAIN	SR	MAIN	SR
Worst Pair	12	12	12	12
RL (dB)	-14.7 F	-13.6 F	-14.7	-13.6
Freq. (MHz)	1.0	1.0	1.0	1.0
Limit (dB)	17.0	17.0	17.0	17.0





* Measurement is within the accuracy limits of the instrument.

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

CERTIFICACIONES MIDENA.flw

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: D1-45

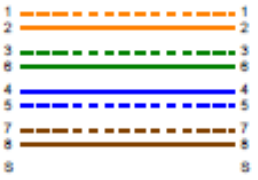
Test Summary: FAIL

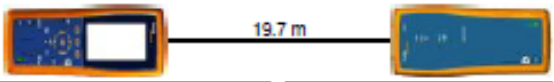
Date / Time:01/24/2010 11:41:08am
Headroom: -0.2 dB (NEXT 12-78)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

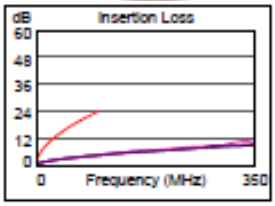
Model: DTX-1800
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
PASS

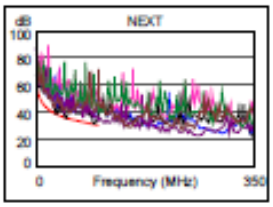


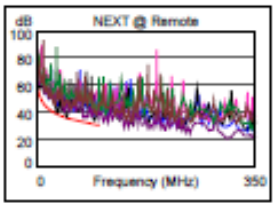


Length (m), Limit 100.0	[Pair 78]	19.7
Prop. Delay (ns), Limit 555		97
Delay Skew (ns), Limit 50		2
Resistance (ohms)	[Pair 12]	3.9
Insertion Loss Margin (dB)	[Pair 36]	19.6
Frequency (MHz)	[Pair 36]	100.0
Limit (dB)	[Pair 36]	24.0

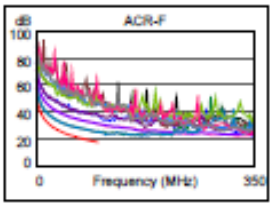


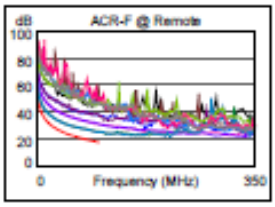
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	12-78	12-78	12-78	12-78
NEXT (dB)	-0.2*F	0.8	0.7	2.7
Freq. (MHz)	47.8	32.8	93.0	92.5
Limit (dB)	35.6	38.4	30.6	30.7
Worst Pair	12	12	12	12
PS NEXT (dB)	1.9	2.6	2.5	4.2
Freq. (MHz)	32.8	32.8	92.8	92.8
Limit (dB)	35.4	35.4	27.6	27.6



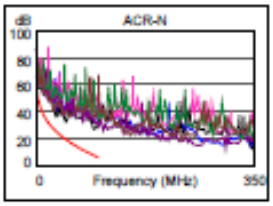


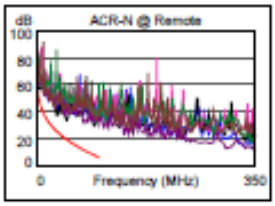
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	45-36	45-36
ACR-F (dB)	6.0	6.0	7.3	7.3
Freq. (MHz)	1.1	1.0	98.3	98.3
Limit (dB)	56.4	57.4	17.6	17.6
Worst Pair	45	45	45	45
PS ACR-F (dB)	8.2	8.2	9.4	9.3
Freq. (MHz)	1.1	1.0	98.0	98.3
Limit (dB)	53.4	54.4	14.6	14.6



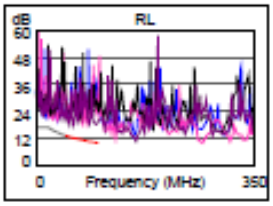


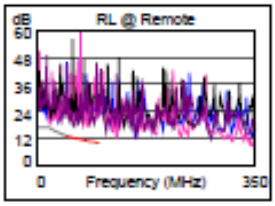
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-78	12-78	12-78	12-78
ACR-N (dB)	5.8	6.0	19.5	21.5
Freq. (MHz)	1.6	2.0	93.0	92.8
Limit (dB)	56.9	55.3	7.5	7.6
Worst Pair	12	12	12	12
PS ACR-N (dB)	8.6	8.6	21.4	23.1
Freq. (MHz)	1.6	2.0	92.8	92.8
Limit (dB)	53.9	52.3	4.6	4.6





PASS	MAIN	SR	MAIN	SR
Worst Pair	78	78	78	78
RL (dB)	5.3	4.7	5.3	4.7
Freq. (MHz)	59.3	59.8	59.3	59.8
Limit (dB)	12.3	12.2	12.3	12.2





* Measurement is within the accuracy limits of the instrument.

LinkWare Version 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

Cable ID: D1-42

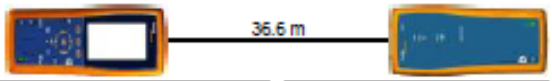
Test Summary: PASS

Date / Time: 01/20/2010 02:55:33pm
Headroom: 4.8 dB (NEXT 36-45)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

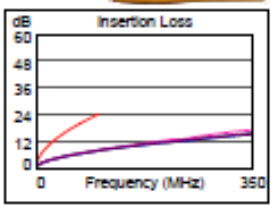
Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

Model: DTX-1800
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

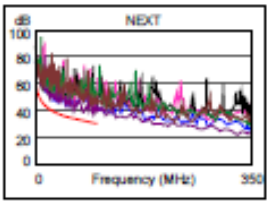
Wire Map (T568B)
PASS

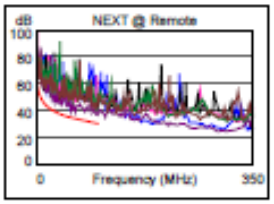


Length (m), Limit 100.0	[Pair 12]	36.6
Prop. Delay (ns), Limit 555		181
Delay Skew (ns), Limit 50		4
Resistance (ohms)	[Pair 12]	6.7
Insertion Loss Margin (dB)	[Pair 36]	16.1
Frequency (MHz)	[Pair 36]	100.0
Limit (dB)	[Pair 36]	24.0

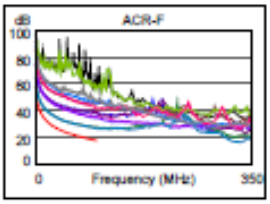


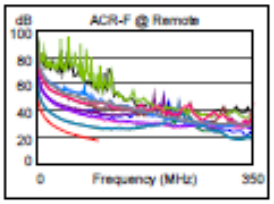
	Worst Case Margin		Worst Case Value	
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	36-45
NEXT (dB)	5.3	4.8	5.3	6.0
Freq. (MHz)	77.8	62.5	78.0	96.8
Limit (dB)	32.0	33.6	31.9	30.3
Worst Pair	36	45	45	45
PS NEXT (dB)	7.7	7.6	8.8	7.6
Freq. (MHz)	62.0	62.5	96.8	96.8
Limit (dB)	30.6	30.6	27.3	27.3



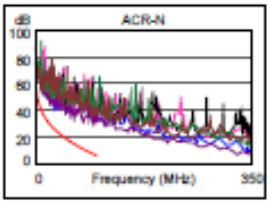


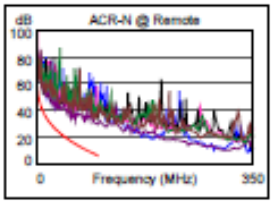
PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	45-36	45-36	36-45
ACR-F (dB)	6.8	6.8	9.0	9.2
Freq. (MHz)	1.0	1.0	98.0	97.8
Limit (dB)	57.4	57.4	17.6	17.6
Worst Pair	45	36	36	45
PS ACR-F (dB)	9.4	9.4	11.6	11.3
Freq. (MHz)	1.0	1.0	98.0	97.8
Limit (dB)	54.4	54.4	14.6	14.6



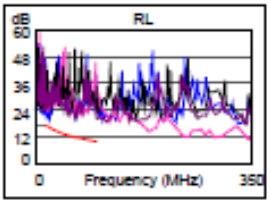


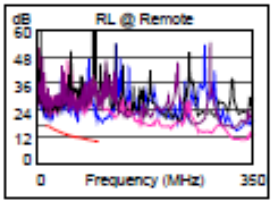
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	36-45	36-45
ACR-N (dB)	14.0	13.9	22.5	22.1
Freq. (MHz)	1.8	1.8	93.3	96.8
Limit (dB)	56.4	56.4	7.5	6.7
Worst Pair	12	12	45	45
PS ACR-N (dB)	14.5	14.3	24.9	23.7
Freq. (MHz)	1.6	1.8	96.8	96.8
Limit (dB)	53.9	53.4	3.7	3.7





PASS	MAIN	SR	MAIN	SR
Worst Pair	12	12	12	12
RL (dB)	3.4	3.2	7.5	7.5
Freq. (MHz)	21.0	21.1	66.8	67.0
Limit (dB)	16.8	16.8	11.8	11.7





Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

LinkWare Version: 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: D1-27

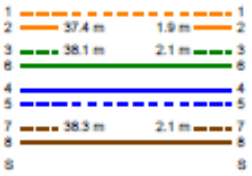
Test Summary: FAIL

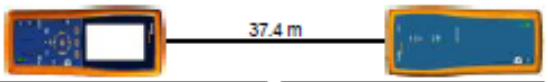
Date / Time: 01/20/2010 03:25:53pm
Headroom: -38.8 dB (NEXT 12-36)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

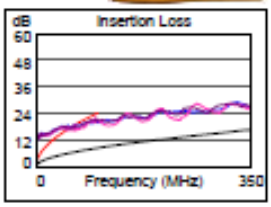
Model: DTX-1800
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
FAIL

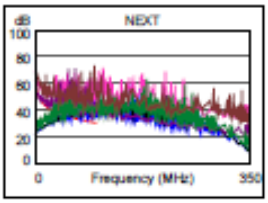


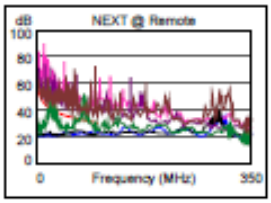


Length (m), Limit 100.0	[Pair 12]	37.4
Prop. Delay (ns), Limit 555		191
Delay Skew (ns), Limit 50		10
Resistance (ohms)	[Pair 12]	Open
Insertion Loss Margin (dB)	[Pair 12]	-10.4 F
Frequency (MHz)	[Pair 12]	1.4
Limit (dB)	[Pair 12]	3.0

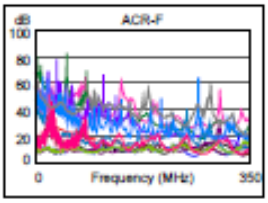


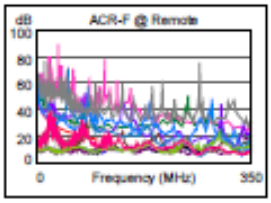
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-36	12-36	12-36
NEXT (dB)	-38.7 F	-38.8 F	-38.7	-26.5
Freq. (MHz)	1.0	1.5	1.0	10.3
Limit (dB)	60.0	60.0	60.0	46.8
Worst Pair	12	12	12	12
PS NEXT (dB)	-38.6 F	-38.7 F	-38.6	-19.3
Freq. (MHz)	1.0	1.5	1.0	27.4
Limit (dB)	57.0	57.0	57.0	36.7



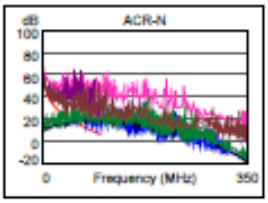


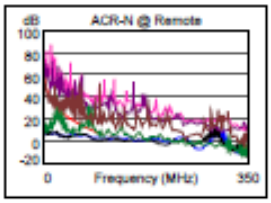
FAIL	MAIN	SR	MAIN	SR
Worst Pair	36-12	36-12	78-12	12-78
ACR-F (dB)	-49.3 F	-48.9 F	-19.1	-11.7
Freq. (MHz)	1.0	1.0	36.8	92.8
Limit (dB)	57.4	57.4	26.1	18.1
Worst Pair	12	12	12	12
PS ACR-F (dB)	-49.2 F	-48.4 F	-18.8	-18.8
Freq. (MHz)	1.0	1.0	36.5	36.8
Limit (dB)	54.4	54.4	23.2	23.1



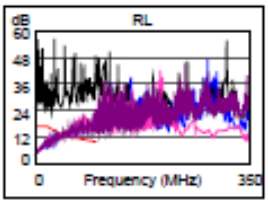


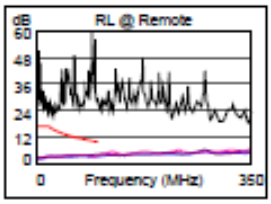
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-36	12-78	12-36	12-78
ACR-N (dB)	-48.5	-48.8	-48.5	-6.8
Freq. (MHz)	1.1	1.5	1.1	95.5
Limit (dB)	57.0	57.0	57.0	7.0
Worst Pair	12	12	12	12
PS ACR-N (dB)	-48.9	-49.0	-48.9	-8.0
Freq. (MHz)	1.1	1.4	1.1	83.8
Limit (dB)	54.0	54.0	54.0	6.6





FAIL	MAIN	SR	MAIN	SR
Worst Pair	12	12	12	12
RL (dB)	-13.4 F	-14.7 F	-13.4	-14.7
Freq. (MHz)	1.0	1.0	1.0	1.0
Limit (dB)	17.0	17.0	17.0	17.0





LinkWare Version 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

CERTIFICACIONES MIDENA.flw

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: D1-26

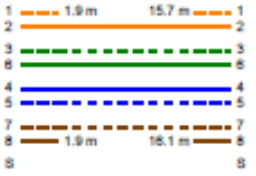
Test Summary: FAIL

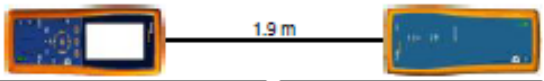
Date / Time:02/12/2010 10:27:31am
Headroom: -42.3 dB (NEXT 12-78)
Test Limit: TIA Cat 6 Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2600
NVP: 69.0%

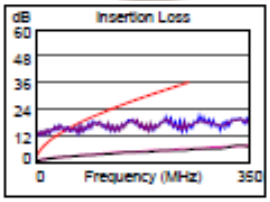
Model: DTX-1600
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
FAIL

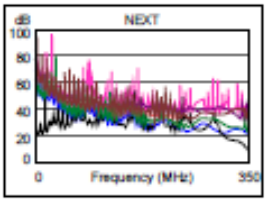


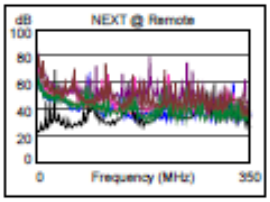


Length (m), Limit 100.0	[Pair 12]	1.9
Prop. Delay (ns), Limit 555		88
Delay Skew (ns), Limit 50		79 F
Resistance (ohms)	[Pair 12]	Open
Insertion Loss Margin (dB)	[Pair 78]	-10.1 F
Frequency (MHz)	[Pair 78]	2.6
Limit (dB)	[Pair 78]	3.3

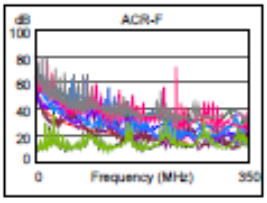


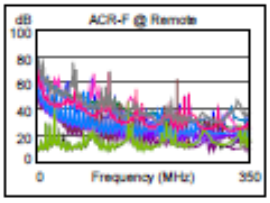
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	12-78	12-78	12-78	12-78
NEXT (dB)	-42.3 F	-42.0 F	-41.0	-39.9
Freq. (MHz)	3.0	2.9	4.8	4.3
Limit (dB)	65.0	65.0	61.8	62.6
Worst Pair	12	12	12	12
PS NEXT (dB)	-39.7 F	-39.1 F	-38.5	-37.4
Freq. (MHz)	3.3	3.1	4.8	4.3
Limit (dB)	62.0	62.0	59.3	60.1



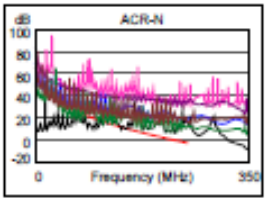


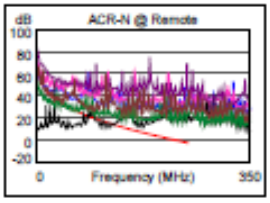
FAIL	MAIN	SR	MAIN	SR
Worst Pair	12-78	12-78	78-12	78-12
ACR-F (dB)	-51.7 F	-51.7 F	-14.0	-10.4
Freq. (MHz)	1.0	1.0	120.5	175.5
Limit (dB)	63.3	63.3	21.6	18.4
Worst Pair	78	12	12	78
PS ACR-F (dB)	-48.7 F	-48.7 F	-11.1	-11.0
Freq. (MHz)	1.0	1.0	120.5	120.5
Limit (dB)	60.3	60.3	18.6	18.6



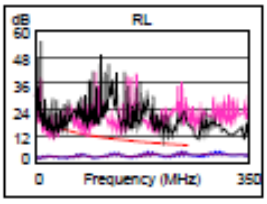


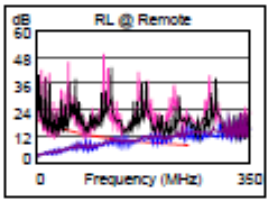
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-78	12-78	12-78	12-78
ACR-N (dB)	-52.3	-52.0	4.5	-51.8
Freq. (MHz)	3.0	2.5	221.0	3.1
Limit (dB)	61.5	61.8	0.6	61.2
Worst Pair	78	78	12	78
PS ACR-N (dB)	-49.6	-49.0	5.0	-49.0
Freq. (MHz)	3.3	2.5	221.0	3.1
Limit (dB)	58.4	58.8	-2.3	58.4





FAIL	MAIN	SR	MAIN	SR
Worst Pair	12	12	12	12
RL (dB)	-17.0 F	-16.4 F	-17.0	-16.4
Freq. (MHz)	2.4	1.0	2.4	1.0
Limit (dB)	19.0	19.0	19.0	19.0





LinkWare Version 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: D1-07

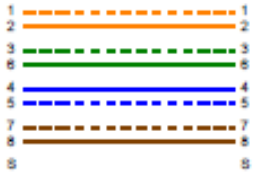
Test Summary: FAIL

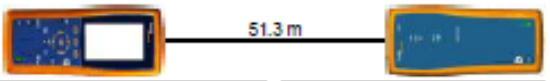
Date / Time: 01/21/2010 08:57:36am
Headroom: -20.3 dB (NEXT 36-45)
Test Limit: TIA Cat 5e Channel
Cable Type: Cat 5e UTP

Operator: NANCY RAMON
Software Version: 2.1200
Limits Version: 1.2800
NVP: 69.0%

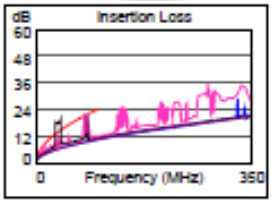
Model: DTX-1600
Main S/N: 9659001
Remote S/N: 9659002
Main Adapter: DTX-CHA001
Remote Adapter: DTX-CHA001

Wire Map (T568B)
PASS

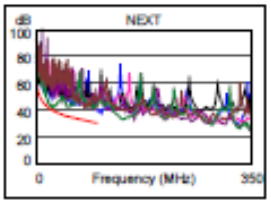


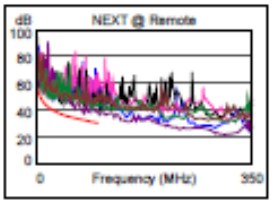


Length (m), Limit 100.0	[Pair 12]	51.3
Prop. Delay (ns), Limit 555		253
Delay Skew (ns), Limit 50		5
Resistance (ohms)	[Pair 45]	45.3
Insertion Loss Margin (dB)	[Pair 45]	-10.3 F
Frequency (MHz)	[Pair 45]	1.1
Limit (dB)	[Pair 45]	3.0

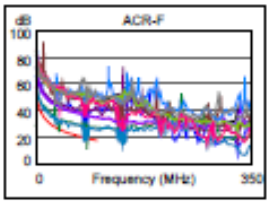


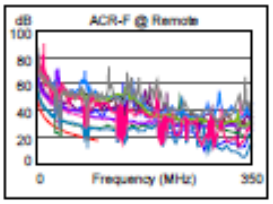
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	36-78	36-45	12-36	36-45
NEXT (dB)	2.0	-20.3 F	8.7	5.2
Freq. (MHz)	26.0	1.0	100.0	77.5
Limit (dB)	40.1	60.0	30.1	32.0
Worst Pair	36	36	12	36
PS NEXT (dB)	4.3	-17.3 F	9.6	9.1
Freq. (MHz)	24.1	1.0	97.8	98.5
Limit (dB)	37.6	57.0	27.2	27.2



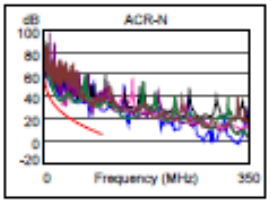


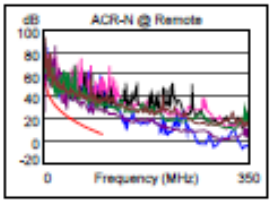
FAIL	MAIN	SR	MAIN	SR
Worst Pair	36-45	45-36	36-45	45-36
ACR-F (dB)	-29.7 F	-19.0 F	-8.2	-7.4
Freq. (MHz)	1.0	1.0	83.5	83.5
Limit (dB)	57.4	57.4	19.0	19.0
Worst Pair	45	36	45	36
PS ACR-F (dB)	-26.7 F	-26.7 F	-5.2	-5.2
Freq. (MHz)	1.0	1.0	83.5	83.5
Limit (dB)	54.4	54.4	16.0	16.0



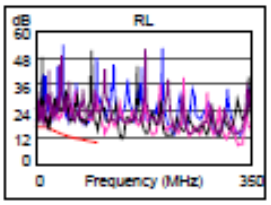


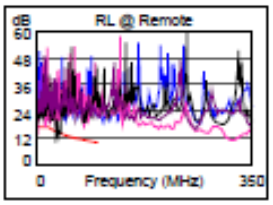
N/A	MAIN	SR	MAIN	SR
Worst Pair	12-36	36-45	12-36	12-36
ACR-N (dB)	7.9	-30.6	10.4	14.3
Freq. (MHz)	3.0	1.0	78.3	78.3
Limit (dB)	51.7	57.0	10.9	10.9
Worst Pair	36	45	36	36
PS ACR-N (dB)	7.5	-27.6	10.3	8.2
Freq. (MHz)	25.1	1.0	78.3	78.3
Limit (dB)	25.8	54.0	7.9	7.9





FAIL	MAIN	SR	MAIN	SR
Worst Pair	45	45	45	45
RL (dB)	0.2"	-12.1 F	6.1	-12.1
Freq. (MHz)	1.0	1.0	100.0	1.0
Limit (dB)	17.0	17.0	10.0	17.0





* Measurement is within the accuracy limits of the instrument.

LinkWare Version 6.2

Project: BLOQUE-1
Site: muestra

FLUKE networks

ANEXO 4. DIRECCIONAMIENTO IP BASADO EN VLAN

Vlan 11: UNIEJE			IP:10.10.10.224 - 10.10.10.255 GATEWAY:10.10.10.225	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.41	10.10.10.226	Unidad Ejecutora	Oficial de Ingeniería	21	D1-21
B1	10.10.9.42	10.10.10.227	Unidad Ejecutora	Oficial de Ingeniería	23	D1-23
B1	10.10.9.43	10.10.10.228	Unidad Ejecutora	Oficial de Ingeniería	24	D1-24
B1	10.10.9.44	10.10.10.229	Unidad Ejecutora	Oficial de Ingeniería	5	D1-25
B1	10.10.9.37	10.10.10.230	Unidad Ejecutora	Operador		V1-26
B1	10.10.9.56	10.10.10.231	Unidad Ejecutora	Operador		V1-29
B1	10.10.9.57	10.10.10.232	Unidad Ejecutora	Supervisor		Alim. AP
B1	10.10.9.68	10.10.10.233	Unidad Ejecutora	Técnico Sección		Alim. AP
B1	10.10.9.69	10.10.10.234	Unidad Ejecutora	Técnico Sección		Alim. AP

Vlan 12: COMU			IP:10.10.11.160 - 10.10.11.175 GATEWAY:10.10.11.161	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.16	10.10.11.162	Departamento de Sistemas/Comunicaciones	Operador	13	D1-13
B1	10.10.9.17	10.10.11.163	Departamento de Sistemas/Comunicaciones	Operador	10	D1-10
B1	10.10.9.18	10.10.11.164	Departamento de Sistemas/Comunicaciones	Supervisor	18	D1-18
B1	10.10.9.19	10.10.11.165	Departamento de Sistemas/Comunicaciones	Jefe de seguridad	1	D1-04
B1	10.10.9.35	10.10.11.166	Departamento de Sistemas/Comunicaciones	Operador		D1-12

Vlan 13: SEGU			IP:10.10.11.176 - 10.10.11.191 GATEWAY:10.10.11.177	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP-ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.50	10.10.11.178	Dirección Administrativa/Seguridad	Supervisor	8	D1-28
B2	10.10.10.66	10.10.11.179	Dirección Administrativa/Seguridad	Inspector Seguridad	20(1)	D1-20
B2	10.10.10.75	10.10.11.180	Dirección Administrativa/Seguridad	Inspector Seguridad	23(1)	D1-21
B2	10.10.10.85	10.10.11.181	Dirección Administrativa/Seguridad	Inspector de Seguridad	11(2)	D2-26
B2	10.10.10.89	10.10.11.182	Dirección Administrativa/Seguridad	Secretaría/Ingreso Documentación		D2-25

Vlan 14: CCTRL			IP:10.10.11.96 - 10.10.11.111 GATEWAY:10.10.11.97	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.10	10.10.11.98	Cuarto de Control	Administrador	3	CD
B1	10.10.9.61	10.10.11.99	Cuarto de Control	Adm. Lectores de Huellas	14	V2-30
B1	10.10.9.62	10.10.11.100	Cuarto de Control	Adm. Lectores de Huellas	15	V2-31
B2	10.10.10.105	10.10.11.101	Cuarto de Control	Control sistemas personal	19(2)	CD
B2	10.10.10.86	10.10.11.102	Puerta de ingreso 2	Lectores de huellas	26(2)	CD
B2	10.10.10.87	10.10.11.103	Puerta de ingreso 2	Lectores de huellas	27(2)	CD

Vlan 15: DIRLOGI			IP:10.10.9.192 - 10.10.9.223 GATEWAY:10.10.9.193	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.23	10.10.9.194	Dirección Logística / Bodega	Abastecimiento	2	D1-02
B3	10.10.11.9	10.10.9.195	Dirección de Logística	Sala de Sesiones		D1-45
B3	10.10.11.10	10.10.9.196	Dirección de Logística	Director	47	D1-47
B3	10.10.11.11	10.10.9.197	Dirección de Logística	Secretaría	44	D1-44

B3	10.10.11.12	10.10.9.198	Dirección de Logística	Sub Director	25	D2-01
B3	10.10.11.13	10.10.9.199	Dirección de Logística	Subdirección, Amanuense	33	D1-33
B3	10.10.11.20	10.10.9.200	Dirección de Logística	Administrativo	28	D1-28
B3	10.10.11.21	10.10.9.201	Dirección de Logística	Asesoría Jurídica	31	D1-31
B3	10.10.11.22	10.10.9.202	Dirección de Logística	Asesoría Jurídica	30	D1-30
B3		10.10.9.203	Dirección de Logística	Sala de Sesiones	.	D1-48
B3		10.10.9.204	Dirección de Logística	Sala de Sesiones	.	D1-43
B3		10.10.9.205	Dirección de Logística	Sala de Sesiones	.	D2-02
B3		10.10.9.206	Dirección de Logística	Sala de Sesiones	.	D2-03
B3	10.10.11.36	10.10.9.207	Dirección de Logística	Jefatura	42	D2-07
B3	10.10.11.37	10.10.9.208	Dirección de Logística	Administración portal	4	D2-04
B3	10.10.11.45	10.10.9.209	Dirección de Logística	Administrativo	3	D2-05

Vlan 16: DEPCON			**IP:10.10.10.32 - 10.10.10.63 GATEWAY:10.10.10.33**	**MASK: 255.255.255.224**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B1	10.10.9.55	10.10.10.34	Departamento de Control	Jefatura	6	D1-06
B1	10.10.9.65	10.10.10.35	Departamento de Control	Operador		D2-21
B1	10.10.9.67	10.10.10.36	Departamento de Control	Secretaría		V1-39
B2	10.10.10.41	10.10.10.37	Departamento de Control	Jefe de Departamento	4(1)	D1-04
B2	10.10.10.42	10.10.10.38	Departamento de Control	Subjefatura	17(1)	D2-17
B2	10.10.10.44	10.10.10.39	Departamento de Control	Sección Técnica	.	D1-03
B2	10.10.10.45	10.10.10.40	Departamento de Control	Administrativo	1(2)	D1-01
B2	10.10.10.47	10.10.10.41	Departamento de Control	Administrativo	14(3)	D1-06
B2	10.10.10.78	10.10.10.42	Departamento de Control	Administrativo	15(1)	D1-15
B2	10.10.10.79	10.10.10.43	Departamento de Control	Administrativo	38(2)	D1-28
B2	10.10.10.101	10.10.10.44	Departamento de Control	Sección Técnica		D1-02
B2	10.10.10.80	10.10.10.45	Departamento de Control	Sala de Sesiones	12(1)	D1-12
B2	10.10.10.81	10.10.10.46	Departamento de Control	Administrativo	10(1)	D1-10

Vlan 17: DIRPER1			IP:10.10.10.0 - 10.10.10.31 GATEWAY:10.10.10.1	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B2	10.10.10.10	10.10.10.2	Dirección de Personal	Director	8(2)	D2-10
B2	10.10.10.11	10.10.10.3	Dirección de Personal	Secretaría Director	33(2)	D2-20
B2	10.10.10.12	10.10.10.4	Dirección de Personal	Subdirector	7(2)	D2-09
B2	10.10.10.14	10.10.10.5	Dirección de Personal	Derechos Humanos	48(1)	D1-48
B2	10.10.10.15	10.10.10.6	Dirección de Personal	Supervisor	3(2)	D2-03
B2	10.10.10.18	10.10.10.7	Dirección de Personal	Pases	47(1)	D1-47
B2	10.10.10.20	10.10.10.8	Dirección de Personal	Estadística	4(2)	D2-01
B2	10.10.10.21	10.10.10.9	Dirección de Personal	Tec. de Archivo	39(1)	D1-39
B2	10.10.10.22	10.10.10.10	Dirección de Personal	Sec. Técnica	36(1)	D1-36
B2	10.10.10.28	10.10.10.11	Dirección de Personal	Oficinista	33(1)	D1-33
B2	10.10.10.29	10.10.10.12	Dirección de Personal	Ast. Administrativo	34(1)	D1-34
B2	10.10.10.36	10.10.10.13	Dirección de Personal	Jefe Dep. Plan Militar	14(1)	D1-14
B2	10.10.10.38	10.10.10.14	Dirección de Personal	Amanuense	17(2)	D2-27
B2	10.10.10.39	10.10.10.15	Dirección de Personal	Escalafón	45(1)	D1-45

Vlan 18: DIRPER2			IP:10.10.10.128 - 10.10.10.159 GATEWAY:10.10.10.129	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B2	10.10.10.23	10.10.10.130	Dirección de Personal	Jefe de Jefatura	37(1)	D1-37
B2	10.10.10.40	10.10.10.131	Dirección de Personal	Ingresos	41(1)	D1-41
B2	10.10.10.24	10.10.10.132	Dirección de Personal	Analista RRHH	38(1)	D1-38
B2	10.10.10.25	10.10.10.133	Dirección de Personal	Analista Financiero	30(1)	D1-30
B2	10.10.10.26	10.10.10.134	Dirección de Personal	Tec. Nomina	31(1)	D1-31
B2	10.10.10.27	10.10.10.135	Dirección de Personal	Ast. RRHH	32(1)	D1-32
B2	10.10.10.31	10.10.10.136	Dirección de Personal	Permisos	43(1)	D1-43
B2	10.10.10.41	10.10.10.137	Dirección de Personal	Sicóloga		D1-18

B2	10.10.10.30	10.10.10.138	Dirección de Personal	Trabajadora Social	19(1)	D1-19
B2	10.10.10.32	10.10.10.139	Dirección de Personal	Sec. Servicio Social	16(1)	D1-17
B2	10.10.10.34	10.10.10.140	Dirección de Personal	Bienestar Psicología	11(1)	D1-16

Vlan 19: ASUINT			**IP:10.10.11.192 - 10.10.11.207 GATEWAY:10.10.11.193**	**MASK: 255.255.255.240**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B2	10.10.10.55	10.10.11.194	Asuntos Internacionales	Jefatura	27(1)	D1-27
B2	10.10.10.56	10.10.11.195	Asuntos Internacionales	Secretaría	25(1)	D1-25
B2	10.10.10.57	10.10.11.196	Asuntos Internacionales	Agregadurías	26(1)	D1-26
B2	10.10.10.58	10.10.11.197	Asuntos Internacionales	Agregadurías	29(1)	D1-29
B2	10.10.10.108	10.10.11.198	Asuntos Internacionales	Administrativo		V1-29

Vlan 20: SREU			**IP:10.10.9.0 - 10.10.9.63 GATEWAY:10.10.9.1**	**MASK: 255.255.255.192**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B2	10.10.10.9	10.10.9.2	Salón Auditorio	Auditorio	24(1)	D1-22
B4		10.10.9.3	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-48
B4		10.10.9.4	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-47
B4		10.10.9.5	Dirección de Telecomunicaciones	Libre/Sala de Reuniones		D1-42
B5		10.10.9.6	Sala de Reuniones	Libre		D1-15
B5		10.10.9.7	Sala de Reuniones	Libre		D1-24
B5		10.10.9.8	Sala de Reuniones	Libre		D1-16
B6	10.10.14.79	10.10.9.9	Dirección de Operaciones	Sala de Reuniones	45	D1-23
B6	10.10.14.80	10.10.9.10	Dirección de Operaciones	Sala de Reuniones		D1-24
B6	10.10.14.81	10.10.9.11	Dirección de Operaciones	Administrativo	36	D1-12
B6	10.10.14.82	10.10.9.12	Dirección de Operaciones	Administrativo	34	D1-19
B6		10.10.9.13	Dirección de Operaciones	Libre		D2-15

Vlan 21: CGRAL			IP:10.10.12.32 - 10.10.12.47 GATEWAY:10.10.12.33	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.23	10.10.12.34	Cuartel General	Planificación	27	D1-27
B3	10.10.11.24	10.10.12.35	Cuartel General	Supervisor	32	D1-38
B3	10.10.11.25	10.10.12.36	Cuartel General	Seguros de Vehículos	26	D1-26
B3	10.10.11.26	10.10.12.37	Cuartel General	Transportes	23	D1-23

Vlan 22: DEPING			IP:10.10.11.32 - 10.10.11.47 GATEWAY:10.10.11.33	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.27	10.10.11.34	Departamento de Ingeniería	Jefatura	21	D1-21
B3	10.10.11.29	10.10.11.35	Departamento de Ingeniería	Obras civiles	20	D1-20
B3	10.10.11.30	10.10.11.36	Departamento de Ingeniería	Obras civiles	15	D1-15
B3	10.10.11.32	10.10.11.37	Departamento de Ingeniería	Planificación	17	D1-17
B3	10.10.11.33	10.10.11.38	Departamento de Ingeniería	Planificación	18	D1-18
B3	10.10.11.34	10.10.11.39	Departamento de Ingeniería	Secretaría	41	D1-41
B3	10.10.11.35	10.10.11.40	Departamento de Ingeniería	Secretaría	39	D1-39
B3		10.10.11.41	Departamento de Ingeniería	Libre		D1-40

Vlan 23: CONPUB			IP:10.10.11.208 - 10.10.11.223 GATEWAY:10.10.11.209	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.38	10.10.11.210	Departamento de Contratación Pública	Operador	45	D2-09
B3	10.10.11.39	10.10.11.211	Departamento de Contratación Pública	Operador	22	D2-14
B3	10.10.11.80	10.10.11.212	Departamento de Contratación Pública	Administrativo	40	D2-15
B3	10.10.11.81	10.10.11.213	Departamento de Contratación Pública	Operador	38	D2-06
B3	10.10.11.43	10.10.11.214	Departamento de Contratación Pública	Administrativo	1	D2-13

Vlan 24: SANIDAD			IP:10.10.9.224 - 10.10.9.255 GATEWAY:10.10.9.225	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.52	10.10.9.225	Dirección de Sanidad	Director	6	D1-06
B3	10.10.11.53	10.10.9.226	Dirección de Sanidad	Subdirector	2	D1-02
B3	10.10.11.54	10.10.9.227	Dirección de Sanidad	Secretaría	8	D1-08
B3	10.10.11.55	10.10.9.228	Dirección de Sanidad	Digitador	7	D1-07
B3	10.10.11.56	10.10.9.229	Dirección de Sanidad	Administrativo	9	D1-09
B3	10.10.11.57	10.10.9.230	Dirección de Sanidad	Jefatura	12	D1-12
B3	10.10.11.58	10.10.9.231	Dirección de Sanidad	Medicina Preventiva	10	D1-10
B3	10.10.11.59	10.10.9.232	Dirección de Sanidad	Dpto. Estadística	11	D1-11
B3	10.10.11.60	10.10.9.233	Dirección de Sanidad	Asistente Planificación	19	D1-19
B3	10.10.11.61	10.10.9.234	Dirección de Sanidad	Jefatura	16	D1-16
B3	10.10.11.62	10.10.9.235	Dirección de Sanidad	Planificación	14	D1-14
B3	10.10.11.63	10.10.9.236	Dirección de Sanidad	Estadísticas	13	D1-13
B3	10.10.11.64	10.10.9.237	Dirección de Sanidad	Libre/Sala de Sesiones		D1-01
B3	10.10.11.65	10.10.9.238	Dirección de Sanidad	Libre		D1-03
B3	10.10.11.66	10.10.9.239	Dirección de Sanidad	Libre		D1-46

Vlan 25: EVACTRL			IP:10.10.11.112 - 10.10.11.127 GATEWAY:10.10.11.113	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.17	10.10.11.114	Departamento de Evaluación y Control	Director	**5**	D1-32
B3	10.10.11.19	10.10.11.115	Departamento de Evaluación y Control	Administrativo	24	D1-34
B6	10.10.14.40	10.10.11.116	Departamento de Evaluación y Control	Jefatura	41	D1-22
B6	10.10.14.42	10.10.11.117	Departamento de Evaluación y Control	Planificación	30	V1-13
B6	10.10.14.43	10.10.11.118	Departamento de Evaluación y Control	Administrativo	9	D2-06
B6		10.10.11.119	Sala de Reuniones	Libre		D1-26

Vlan 26: DIRTEL			IP:10.10.9.160 - 10.10.9.191 GATEWAY:10.10.9.161	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.10	10.10.9.162	Dirección de Telecomunicaciones	Director	43(1)	D1-43
B4	10.10.12.11	10.10.9.163	Dirección de Telecomunicaciones	Secretaría	46(1)	D1-46
B4	10.10.12.12	10.10.9.164	Dirección de Telecomunicaciones	Dpto. Control y Evaluación	16(2)	V1-44
B4	10.10.12.13	10.10.9.165	Dirección de Telecomunicaciones	Administrativo	37(1)	D1-37
B4	10.10.12.14	10.10.9.166	Dirección de Telecomunicaciones	Administrativo	39(1)	D1-39
B4	10.10.12.15	10.10.9.167	Dirección de Telecomunicaciones	Administrativo	41(1)	D1-41
B4	10.10.12.17	10.10.9.168	Dirección de Telecomunicaciones	Jefatura	38(1)	D1-38
B4	10.10.12.18	10.10.9.169	Dirección de Telecomunicaciones	Activos Fijos	17(1)	D1-35
B4	10.10.12.19	10.10.9.170	Dirección de Telecomunicaciones	Administrativo	34(1)	D1-34
B4	10.10.12.20	10.10.9.171	Dirección de Telecomunicaciones	Presupuesto	9(1)	D1-33
B4	10.10.12.25	10.10.9.172	Dirección de Telecomunicaciones	Administrativo	40(1)	D1-40
B4	10.10.12.26	10.10.9.173	Dirección de Telecomunicaciones	Jefatura	28(1)	D1-28
B4	10.10.12.28	10.10.9.174	Dirección de Telecomunicaciones	Administrativo	27(1)	D1-27
B4	10.10.12.30	10.10.9.175	Dirección de Telecomunicaciones	Administrativo	29(1)	D1-29
B4	10.10.12.31	10.10.9.176	Dirección de Telecomunicaciones	Secretaría	30(1)	D1-30
B4	10.10.12.33	10.10.9.177	Dirección de Telecomunicaciones	Jefatura	25(1)	D1-25
B4	10.10.12.34	10.10.9.178	Dirección de Telecomunicaciones	Administrativo	31(1)	D1-31
B4	10.10.12.36	10.10.9.179	Dirección de Telecomunicaciones	Administrativo	32(1)	D1-32

Vlan 27: DIRSIST1			IP:10.10.10.96 - 10.10.10.127 GATEWAY:10.10.10.97	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.23	10.10.10.98	Dirección de Sistemas	Director		D1-44
B4	10.10.12.48	10.10.10.99	Dirección de Sistemas	Amanuense	45(1)	D1-45
B4	10.10.12.121	10.10.10.100	Dirección de Sistemas	Administrativo	2(2)	D2-27
B4	10.10.12.122	10.10.10.101	Dirección de Sistemas	Administrativo	11(2)	D2-28

B4	10.10.12.123	10.10.10.102	Dirección de Sistemas	Supervisor	28(2)	D2-29
B4	10.10.12.124	10.10.10.103	Dirección de Sistemas	Planificador	3(2)	D2-30
B4	10.10.12.125	10.10.10.104	Dirección de Sistemas	Planificador	38(2)	D2-31
B4	10.10.12.126	10.10.10.105	Dirección de Sistemas	Amanuense	14(2)	D2-32
B4	10.10.12.127	10.10.10.106	Dirección de Sistemas	Planificador	26(2)	V1-33
B4	10.10.12.129	10.10.10.107	Dirección de Sistemas	Director	31(2)	D2-20
B4	10.10.12.142	10.10.10.108	Dirección de Sistemas	Administrativo	26(1)	D1-26

Vlan 28: DIRSIST2			**IP:10.10.10.64 - 10.10.10.95 GATEWAY:10.10.10.65**	**MASK: 255.255.255.224**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.49	10.10.10.66	Dirección de Sistemas	Jefatura	7(2)	D2-11
B4	10.10.12.50	10.10.10.67	Dirección de Sistemas	Secretaría	9(2)	D2-10
B4	10.10.12.52	10.10.10.68	Dirección de Sistemas	Supervisor	35(2)	D2-25
B4	10.10.12.53	10.10.10.69	Dirección de Sistemas	Planificador	5(2)	D2-07
B4	10.10.12.54	10.10.10.70	Dirección de Sistemas	Suministros	37(2)	D2-13
B4	10.10.12.56	10.10.10.71	Dirección de Sistemas	Sala de Reuniones	12(2)	D2-09
B4	10.10.12.60	10.10.10.72	Dirección de Sistemas	Técnico Soporte	4(2)	D2-05
B4	10.10.12.67	10.10.10.73	Dirección de Sistemas	Técnico Soporte	22(2)	D2-06
B4	10.10.12.74	10.10.10.74	Dirección de Sistemas	Técnico Soporte	.	D2-17
B4	10.10.12.120	10.10.10.75	Dirección de Sistemas	Desarrollador	6(2)	D2-26
B4	10.10.12.138	10.10.10.76	Dirección de Sistemas	Desarrollador	32(2)	D2-22
B4	10.10.12.139	10.10.10.77	Dirección de Sistemas	Desarrollador	34(2)	D2-23
B4	10.10.12.140	10.10.10.78	Dirección de Sistemas	Desarrollador	10(2)	D2-24

Vlan 29: DIRSIST3			IP:10.10.11.64 - 10.10.11.79 GATEWAY:10.10.11.65	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.131	10.10.11.66	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.132	10.10.11.67	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.133	10.10.11.68	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.134	10.10.11.69	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.135	10.10.11.70	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.136	10.10.11.71	Dirección de Sistemas	Técnico Soporte		sw inf
B4	10.10.12.141	10.10.11.72	Dirección de Sistemas	Técnico Soporte		sw inf

Vlan 30: ADMIN			IP:10.10.12.64 - 10.10.12.71 GATEWAY:10.10.12.65	MASK: 255.255.255.248		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.51	10.10.12.66	Dirección de Sistemas	Técnico Redes		D2-08
B4	10.10.12.137	10.10.12.67	Dirección de Sistemas	Supervisor Redes	33(2)	D2-21
B4	10.10.12.143	10.10.12.68	Dirección de Sistemas	Técnico Soporte	40(2)	V2-12

Vlan 31: DIRADM1			IP:10.10.11.48 - 10.10.11.63 GATEWAY:10.10.11.49	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B3	10.10.11.14	10.10.11.50	Dirección Administrativa	Director	36	D1-36
B3	10.10.11.16	10.10.11.51	Dirección Administrativa	Administrativo	35	D1-35
B3	10.10.11.18	10.10.11.52	Dirección Administrativa	Secretaría	37	D1-37
B4	10.10.12.97	10.10.11.53	Dirección Administrativa-Finanzas	Activos Fijos	16(1)	D1-16
B4	10.10.12.116	10.10.11.54	Dirección Administrativa-Finanzas	Activos Fijos	19(1)	D1-19
B4	10.10.12.119	10.10.11.55	Dirección Administrativa-Finanzas	Administrativo	.	V1-05

B4	10.10.12.120	10.10.11.56	Dirección Administrativa-Finanzas	Administrativo	18(1)	D1-17
B4	10.10.12.128	10.10.11.57	Dirección Administrativa-Finanzas	Planificador	25(2)	V1-11

Vlan 32: DIRADM2			**IP:10.10.9.128 - 10.10.9.159 GATEWAY:10.10.9.129**	**MASK: 255.255.255.224**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.81	10.10.9.130	Dirección Administrativa-Finanzas	Subdirector	1(1)	D1-01
B4	10.10.12.82	10.10.9.131	Dirección Administrativa-Finanzas	Secretaría	6(1)	D1-06
B4	10.10.12.85	10.10.9.132	Dirección Administrativa-Finanzas	Contabilidad	4(1)	D1-04
B4	10.10.12.86	10.10.9.133	Dirección Administrativa-Finanzas	Contabilidad	8(1)	D1-08
B4	10.10.12.87	10.10.9.134	Dirección Administrativa-Finanzas	Contabilidad	12(1)	D1-09
B4	10.10.12.90	10.10.9.135	Dirección Administrativa-Finanzas	Contabilidad	10(1)	D1-10
B4	10.10.12.91	10.10.9.136	Dirección Administrativa-Finanzas	Jefatura	21(1)	D1-21
B4	10.10.12.93	10.10.9.137	Dirección Administrativa-Finanzas	Presupuesto	20(1)	D1-20
B4	10.10.12.94	10.10.9.138	Dirección Administrativa-Finanzas	Presupuesto	15(1)	D1-15
B4	10.10.12.95	10.10.9.139	Dirección Administrativa-Finanzas	Presupuesto	14(1)	D1-14
B4	10.10.12.98	10.10.9.140	Dirección Administrativa-Finanzas	Subjefatura	2(1)	D1-02
B4	10.10.12.99	10.10.9.141	Dirección Administrativa-Finanzas	Presupuesto	11(1)	D1-11
B4	10.10.12.100	10.10.9.142	Dirección Administrativa-Finanzas	Presupuesto	13(2)	D1-12
B4	10.10.12.107	10.10.9.143	Dirección Administrativa-Finanzas	Administrativo	5(1)	D1-05
B4	10.10.12.108	10.10.9.144	Dirección Administrativa-Finanzas	Administrativo	18(2)	D1-18
B2	10.10.10.67	10.10.9.145	Departamento de Pagaduría	Asistente mensajería	22(1)	D2-22
B2	10.10.10.69	10.10.9.146	Departamento de Pagaduría	Tesorería	21(1)	D2-21
B2	10.10.10.82	10.10.9.147	Departamento de Pagaduría	Administrativo	2(1)	V2-26
B2	10.10.10.83	10.10.9.148	Departamento de Pagaduría	Secretaría	3(1)	V2-27

Vlan 33: JURIDICO			IP:10.10.11.80 - 10.10.11.95 GATEWAY:10.10.11.81	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4	10.10.12.9	10.10.11.82	Dirección de Telecomunicaciones	**Asesoría jurídica**	**29(2)**	D2-03
B4	10.10.12.117	10.10.11.83	Comité de Contrataciones	Amanuense		D2-01
B4	10.10.12.118	10.10.11.84	Comité de Contrataciones	Jefatura	1(2)	D2-02
B5	10.10.13.32	10.10.11.85	Asesoría Jurídica	Amanuense	9	D1-09
B5	10.10.13.33	10.10.11.86	Asesoría Jurídica	Amanuense	4	D1-07
B5		10.10.11.87	Asesoría Jurídica	Libre		D1-08
B5		10.10.11.88	Asesoría Jurídica	Libre		D1-19

Vlan 34: JEFATURA1			IP:10.10.10.192 - 10.10.10.223 GATEWAY:10.10.10.193	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B5	10.10.13.10	10.10.10.194	Jefatura	Jefatura	18	D1-18
B5	10.10.13.11	10.10.10.195	Jefatura	Oficial Ayudante	23	D1-23
B5	10.10.13.12	10.10.10.196	Jefatura	Secretaría	21	D1-21
B5	10.10.13.13	10.10.10.197	Jefatura	Amanuense	20	D1-20
B5	10.10.13.54	10.10.10.198	Jefatura	Sala de Reuniones	22	V1-22
B5	10.10.13.14	10.10.10.199	Secretaría General	Jefatura	14	D1-14
B5	10.10.13.15	10.10.10.200	Secretaría General	Asesoría Especializada	10	D1-10
B5	10.10.13.17	10.10.10.201	Secretaría General	Administrativo	13	D1-13
B5	10.10.13.18	10.10.10.202	Secretaría General	Administrativo	12	D1-11
B5	10.10.13.19	10.10.10.203	Secretaría General	Administrativo	8	D1-12

Vlan 35: JEFATURA2			IP:10.10.11.224 - 10.10.11.239 GATEWAY:10.10.11.225	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B5	10.10.13.24	10.10.11.226	Jefatura Estado Mayor	Jefatura	28	D1-28
B5	10.10.13.25	10.10.11.227	Jefatura Estado Mayor	Oficial Ayudante	25	D1-25
B5	10.10.13.26	10.10.11.228	Jefatura Estado Mayor	Secretaría	39	V1-38
B5	10.10.13.27	10.10.11.229	Jefatura Estado Mayor	Amanuense	30	D1-30
B5		10.10.11.230	Sala de Estado Mayor	Sala Reuniones		V1-20

Vlan 36: INTNAC			IP:10.10.11.240 - 10.10.11.255 GATEWAY:10.10.11.241	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B5	10.10.13.28	10.10.11.242	Intereses Nacionales	Jefatura	1	D1-01
B5	10.10.13.29	10.10.11.243	Intereses Nacionales	Secretaría	2	D1-02
B5	10.10.13.30	10.10.11.244	Intereses Nacionales	Administrativo	3	D1-03
B5	10.10.13.31	10.10.11.245	Intereses Nacionales	Asesoría Especializada	5	D1-05
B5		10.10.11.246	Intereses Nacionales	Libre/Comité Asesor		D1-04

Vlan 37: DESAINST			IP:10.10.9.64 - 10.10.9.127 GATEWAY:10.10.9.65	MASK: 255.255.255.192		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B5	10.10.13.38	10.10.9.66	Dirección de Desarrollo Institucional	Jefatura	35	D1-35
B5	10.10.13.39	10.10.9.67	Dirección de Desarrollo Institucional	Secretaría	36	D1-36
B5	10.10.13.40	10.10.9.68	Dirección de Desarrollo Institucional	Asesoría Naval	38	D1-38
B5	10.10.13.41	10.10.9.69	Dirección de Desarrollo Institucional	Amanuense	42	D1-42
B5	10.10.13.42	10.10.9.70	Dirección de Desarrollo Institucional	Asesor civil	41	D1-41
B5	10.10.13.43	10.10.9.71	Dirección de Desarrollo Institucional	Sala de Reuniones	43	D1-43

B5	10.10.13.45	10.10.9.72	Dirección de Desarrollo Institucional	Asesor Aéreo	33	D1-33
B5	10.10.13.46	10.10.9.73	Dirección de Desarrollo Institucional	Amanuense	31	D1-31
B5	10.10.13.47	10.10.9.74	Dirección de Desarrollo Institucional	Administrativo	7	D1-40
B5	10.10.13.53	10.10.9.75	Dirección de Planificación POA	Analista financiero	48	D1-48
B5	10.10.13.50	10.10.9.76	Dirección de Desarrollo Institucional	Asesoría Especializada	37	V2-19
B5	10.10.13.51	10.10.9.77	Dirección de Desarrollo Institucional	Administrativo	44	V2-20
B5	10.10.13.52	10.10.9.78	Dirección de Desarrollo Institucional	Administrativo	34	D1-34
B5		10.10.9.79	Dirección de Desarrollo Institucional	Libre/Sala de Reuniones	.	D1-45
B5		10.10.9.80	Dirección de Desarrollo Institucional	Libre/Sala de Reuniones	.	D1-46
B5	10.10.13.53	10.10.9.81	Dirección de Desarrollo Institucional	Administrativo	26	V2-17
B5	10.10.13.56	10.10.9.82	Dirección de Desarrollo Institucional	Administrativo	32	D1-32
B5	10.10.13.57	10.10.9.83	Dirección de Planificación	Administrativo	16	V2-18
B6	10.10.14.14	10.10.9.84	Dirección de Desarrollo Institucional	Director	15	D1-34
B6	10.10.14.15	10.10.9.85	Dirección de Desarrollo Institucional	Secretaria	17	D1-35

Vlan 38: DIROPE			**IP:10.10.12.0 - 10.10.12.15 GATEWAY:10.10.12.1**	**MASK: 255.255.255.240**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.10	10.10.12.2	Dirección de Operaciones	Dirección	46	D1-28
B6	10.10.14.11	10.10.12.3	Dirección de Operaciones	Subdirector	44	D1-29
B6	10.10.14.12	10.10.12.4	Dirección de Operaciones	Secretaria		D1-31
B6	10.10.14.13	10.10.12.5	Dirección de Operaciones	Administrativo	19	D1-37
B6	10.10.14.16	10.10.12.6	Dirección de Operaciones	Planificación	2	D2-02

Vlan 39: COOPINTER			IP:10.10.11.128 - 10.10.11.143 GATEWAY:10.10.11.129	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.21	10.10.11.130	Dirección de Cooperación Interinstitucional	Jefatura	5	D1-06
B6	10.10.14.22	10.10.11.131	Dirección de Cooperación Interinstitucional	Coordinación		CD
B6	10.10.14.24	10.10.11.132	Dirección de Cooperación Interinstitucional	Misiones de Paz	40	D1-07
B6	10.10.14.25	10.10.11.133	Dirección de Cooperación Interinstitucional	Secretaria	12	D2-21
B6	10.10.14.26	10.10.11.134	Dirección de Cooperación Interinstitucional	Amanuense	39	D1-09
B6	10.10.14.27	10.10.11.135	Dirección de Cooperación Interinstitucional	Misiones de Paz	32	V1-10

Vlan 40: DOCTRINA			IP:10.10.12.16 - 10.10.12.31 GATEWAY:10.10.12.17	MASK: 255.255.255.240		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.32	10.10.12.18	Dirección de Doctrina Conjunta y Educación	Jefatura	33	D1-10
B6	10.10.14.33	10.10.12.19	Dirección de Doctrina Conjunta y Educación	Secretaria	25	D1-15
B6	10.10.14.34	10.10.12.20	Dirección de Doctrina Conjunta y Educación	Administrativo	47	D2-04
B6	10.10.14.36	10.10.12.21	Dirección de Doctrina Conjunta y Educación	Administrativo	11	D2-19
B6	10.10.14.38	10.10.12.22	Dirección de Doctrina Conjunta y Educación	Coordinación	14	D2-20

Vlan 41: PLANORD			IP:10.10.10.160 - 10.10.10.191 GATEWAY:10.10.10.161	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.45	10.10.10.162	Departamento de Planes y Ordenes	Subjefatura	42	D1-11
B6	10.10.14.46	10.10.10.163	Departamento de Planes y Ordenes	Administrativo	10	D2-08
B6	10.10.14.47	10.10.10.164	Departamento de Planes y Ordenes	Administrativo	28	D2-13
B6	10.10.14.48	10.10.10.165	Departamento de Planes y Ordenes	Administrativo	27	D2-14
B6	10.10.14.49	10.10.10.166	Departamento de Planes y Ordenes	Asesor	26	D2-16

B6	10.10.14.51	10.10.10.167	Departamento de Planes y Ordenes	Amanuense	37	D1-08
B6	10.10.14.52	10.10.10.168	Departamento de Planes y Ordenes	Amanuense	.	D1-20
B6	10.10.14.75	10.10.10.169	Departamento de Planes y Ordenes	Jefatura	21	D1-39
B6	10.10.14.76	10.10.10.170	Departamento de Planes y Ordenes	Amanuense	31	V1-40
B6	10.10.14.77	10.10.10.171	Departamento de Planes y Ordenes	Planificación	8	D1-38
B6	10.10.14.78	10.10.10.172	Departamento de Planes y Ordenes	Control	13	D1-36

Vlan 42: FEDDEP			**IP:10.10.11.144 - 10.10.11.159 GATEWAY:10.10.11.145**	**MASK: 255.255.255.240**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.57	10.10.11.146	Federación deportiva	Jefatura	1	D1-01
B6	10.10.14.58	10.10.11.147	Federación deportiva	Administrativo	6	D1-02
B6	10.10.14.59	10.10.11.148	Federación deportiva	Administrativo	4	D1-04
B6	10.10.14.60	10.10.11.149	Federación deportiva	Administrativo	7	D1-03
B6	10.10.14.62	10.10.11.150	Federación deportiva	Amanuense	16	D2-22
B6	10.10.14.63	10.10.11.151	Federación deportiva	Administrativo	46	D1-28

Vlan 43: COMSOC			**IP:10.10.12.48 - 10.10.12.63 GATEWAY:10.10.12.49**	**MASK: 255.255.255.240**		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B6	10.10.14.67	10.10.12.50	Departamento de Comunicación Social	Jefatura	18	D1-40
B6	10.10.14.69	10.10.12.51	Departamento de Comunicación Social	Administrativo	20	D1-42
B6	10.10.14.72	10.10.12.52	Departamento de Comunicación Social	Inst AP Wireless	24	D1-41
B6	10.10.14.73	10.10.12.53	Departamento de Comunicación Social	Supervisor		D1-43

Vlan 44: DIRINV			IP:10.10.11.0 - 10.10.11.31 GATEWAY:10.10.11.1	MASK: 255.255.255.224		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B7	10.101.35.10	10.10.11.2	Dirección de Investigación	Administrativo	1	D1-02
B7	10.101.35.11	10.10.11.3	Dirección de Investigación	Técnico Soporte	2	D1-03
B7	10.101.35.12	10.10.11.4	Dirección de Investigación	Administrativo	3	D1-04
B7	10.101.35.13	10.10.11.5	Dirección de Investigación	Suministros	4	D1-05
B7	10.101.35.14	10.10.11.6	Dirección de Investigación	Administrativo	5	D1-06
B7	10.101.35.15	10.10.11.7	Dirección de Investigación	Técnico Soporte	6	D1-07
B7	10.101.35.16	10.10.11.8	Dirección de Investigación	Administrativo	7	D1-08
B7	10.101.35.17	10.10.11.9	Dirección de Investigación	Planificación	8	D1-09
B7	10.101.35.18	10.10.11.10	Dirección de Investigación	Planificación	9	D1-10

Vlan 45: WIRELESS			IP:10.10.13.0 - 10.10.13.255 GATEWAY:10.10.13.1	MASK: 255.255.255.0		
BLOQUE	**DIRECCIÓN IP - ANTIGUA**	**DIRECCIÓN IP - NUEVA**	**DEPENDENCIA**	**CARGO-USUARIO**	**PUERTO SW**	**TOMA**
B4			Servicio Wireless			

ANEXO 5. CONFIGURACIONES REALIZADAS

SWITCH 5500G

```
#
 sysname cconmuta // nombre del equipo
#
 undo password-control aging enable
 undo password-control length enable
 undo password-control history enable
 password-control login-attempt 3 exceed lock-time 120 // número máximo de intentos permitidos para logueo
#
 local-server nas-ip 127.0.0.1 key 3com
#
 port-security enable // habilitación de seguridad a nivel de puerto
#
 igmp-snooping enable
# // declaración de usuarios
local-user admin //usuario administrador
 password cipher N5'*a`Q37^/P!U*2YH4#GQ!! // password cifrado para usuario administrador
 service-type ssh telnet terminal // habilitación por acceso ssh
 level 3 //determinación del nivel de acceso
local-user manager // declaración usuario manager
 password cipher ]Ma+:,4P)HR$L<a#$_Ra[1!! // password cifrado para usuario manager
 service-type ssh telnet terminal // habilitación por acceso ssh
 level 1 //determinación del nivel de acceso
local-user monitor // declaración usuario monitor
 password cipher ]Ma+:,4P)HR$L<a#$_Ra[1!! // password cifrado para usuario monitor
 service-type ssh telnet terminal // habilitación por acceso ssh
 level 1 //determinación del nivel de acceso
#
acl number 2800  // declaración de acl básica
 rule 0 deny source 10.51.10.0 0.0.0.255 //creación de regla para negar el tráfico de la red
#
acl number 2900 // declaración de acl básica
 rule 0 permit source 10.10.22.0 0.0.0.7 //creación de regla para permitir el tráfico de la subred
 rule 1 deny //creación de regla para negar todo el tráfico
#
acl number 3800 // declaración de acl avanzada
 rule 1 permit ip source 10.51.10.24 0.0.0.7 destination 10.51.10.24 0.0.0.7 //creación de reglas para permitir el tráfico entre miembros de la subred
 rule 2 permit ip source 10.51.10.32 0.0.0.7 destination 10.51.10.32 0.0.0.7
 rule 3 permit ip source 10.51.10.40 0.0.0.7 destination 10.51.10.40 0.0.0.7
```

```
 rule 4 permit ip source 10.51.10.48 0.0.0.7 destination 10.51.10.48 0.0.0.7
 rule 5 permit ip source 10.51.10.56 0.0.0.7 destination 10.51.10.56 0.0.0.7
 rule 6 permit ip source 10.51.10.64 0.0.0.7 destination 10.51.10.64 0.0.0.7
 rule 7 permit ip source 10.51.10.72 0.0.0.7 destination 10.51.10.72 0.0.0.7
 rule 8 permit ip source 10.51.10.80 0.0.0.7 destination 10.51.10.80 0.0.0.7
 rule 9 permit ip source 10.51.10.88 0.0.0.7 destination 10.51.10.88 0.0.0.7
#
vlan 1 //descripción del ID de Vlan
 description VLAN MNGR //descripción de la vlan
#
vlan 2
 description VLAN ENTE1
#
vlan 3
 description VLAN ENTE2
#
vlan 4
 description VLAN ENTE3
#
vlan 5
 description VLAN ENTE4
#
vlan 6
 description VLAN ENTE5
#
vlan 7
 description VLAN ENTE6
#
vlan 8
description VLAN CTRL
#
vlan 9
 description VLAN INVES
#
vlan 10
 description VLAN COMU
#
vlan 11
 description VLAN ADM
#
interface Vlan-interface1 //interface de la Vlan
 ip address 10.51.10.1 255.255.255.248 // direccionamiento IP asignado a la vlan
#
interface Vlan-interface2
 description ENTE1
 ip address 10.51.10.25 255.255.255.248
#
interface Vlan-interface3
 description ENTE2
```

```
 ip address 10.51.10.33 255.255.255.248
#
interface Vlan-interface4
 description ENTE3
 ip address 10.51.10.41 255.255.255.248
#
interface Vlan-interface5
 description ENTE4
 ip address 10.51.10.49 255.255.255.248
#
interface Vlan-interface6
 description ENTE5
 ip address 10.51.10.57 255.255.255.248
#
interface Vlan-interface7
 description ENTE6
 ip address 10.51.10.65 255.255.255.248
#
interface Vlan-interface8
 description CTRL
 ip address 10.51.10.73 255.255.255.248
#
interface Vlan-interface9
 description INVES
 ip address 10.51.10.81 255.255.255.248
#
interface Vlan-interface10
 description COMU
 ip address 10.51.10.89 255.255.255.248
#
interface Vlan-interface11
 description ADM
 ip address 10.10.22.1 255.255.255.248
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1 //interface del puerto de conexión
 stp edged-port enable //habilitación de Spanning Tree
 broadcast-suppression pps 3000 // tiempo de supresión de tormentas de broadcast
 port access vlan 11 // declaración de puerto tipo acceso en vlan 11
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/2 //interface del puerto de conexión
 description Ente1 //descripción asociada a la interfaz de conexión
 stp edged-port enable //habilitación de Spanning Tree
 broadcast-suppression pps 3000 // tiempo de supresión de tormentas de broadcast
```

```
 port access vlan 2 // declaración de puerto tipo acceso en vlan 2
 packet-filter inbound ip-group 2800 rule 0 //habilitación de regla de filtrado en la entrada de tráfico
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/3
 description Ente2
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 3
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/4
 description Ente3
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 4
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
```

```
 apply qos-profile default
#
interface GigabitEthernet1/0/5
 description Ente4
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 5
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/6
 description Ente5
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 6
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/7
 description Ente6
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 7
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
```

```
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/8
 description Ctrl
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 8
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/9
 description Inves
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 9
 packet-filter inbound ip-group 2800 rule 0
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/10
 description Comu
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 10
 packet-filter inbound ip-group 2800 rule 0
```

```
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6
 packet-filter inbound ip-group 3800 rule 7
 packet-filter inbound ip-group 3800 rule 8
 packet-filter inbound ip-group 3800 rule 9
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/11
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown // Puerto deshabilitado
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/12
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/13
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/14
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/15
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/16
 stp edged-port enable
```

```
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/17
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/18
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/19
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/20
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/21
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/22
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/23
 stp edged-port enable
```

```
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/24
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/25
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/26
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/27
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/0/28
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default
#
interface GigabitEthernet1/1/1
#
interface GigabitEthernet1/1/2
#
interface GigabitEthernet1/1/3
#
interface GigabitEthernet1/1/4
#
interface GigabitEthernet1/1/5
```

```
#
interface GigabitEthernet1/1/6
#
interface GigabitEthernet1/1/7
#
interface GigabitEthernet1/1/8
#
interface Cascade1/2/1
#
interface Cascade1/2/2
#
interface NULL0
#
ospf 1 //declaración del protocolo de enrutamiento
 area 0.0.0.1 // declaración del ID área ospf
  network 10.51.10.24 0.0.0.7 //declaración de redes
 area 0.0.0.2
  network 10.51.10.32 0.0.0.7
 area 0.0.0.3
  network 10.51.10.40 0.0.0.7
 area 0.0.0.0
  network 10.51.10.48 0.0.0.7
 area 0.0.0.4
  network 10.51.10.56 0.0.0.7
 area 0.0.0.5
  network 10.51.10.64 0.0.0.7
 area 0.0.0.6
  network 10.51.10.72 0.0.0.7
 area 0.0.0.7
  network 10.51.10.80 0.0.0.7
 area 0.0.0.8
  network 10.51.10.88 0.0.0.7
#
 ip route-static 0.0.0.0 0.0.0.0 201.218.X.X preference 60 //ruta de ruteo por
defecto
# //habilitación de SNMP
 snmp-agent
 snmp-agent local-engineid 8000002B001EC1E3C8806877
 snmp-agent community read public
 snmp-agent sys-info version all
# // habilitación del protocolo SSH
 ssh user admin authentication-type password
 ssh user admin service-type stelnet
# // creación del banner de bienvenida
 header login %(( SWITCH 5500G- CONMUTACION -- ACCESO RESTRINGIDO
))%
#
user-interface aux 0 7 //detalle de la interface aux 0 7
 authentication-mode scheme  // declaración del método de autenticación
```

```
user-interface vty 0 4 //detalle de la interface vty 0 4
 acl 2900 inbound // habilitación de ACL asignada a la interfaz
 authentication-mode scheme  // declaración del método de autenticación
protocol inbound ssh //habilitación del protocolo ssh
#
return
```

SWITCH 3COM 7700

```
#
 sysname CORE7750 // nombre del equipo
#
password-control login-attempt 3 exceed lock-time 120 // número máximo de intentos permitidos para logueo
#
 local-server nas-ip 127.0.0.1 key 3com
#
 domain default enable system
#
 router id 1.1.1.162
#
 temperature-limit 0 10 80
 temperature-limit 1 10 80
 temperature-limit 2 10 80
#
 poe power max-value 2400
# // declaración de usuarios
 local-user admin //usuario administrador
 password cipher NF5a`Q37^/TEU*3TH4#GQH2 // password cifrado para usuario administrador
 service-type lan-access // declaración del tipo de acceso a la lan
 service-type ssh telnet terminal
 level 3 //determinación del nivel de acceso
local-user manager
local-user monitor
#
acl number 2900 // declaración de acl básica
 rule 0 permit source 10.10.22.0 0.0.0.7 //creación de regla para permitir el tráfico de la subred
 rule 1 deny //creación de regla para negar todo el tráfico
#
vlan 1 //descripción del ID de Vlan
description SERVIDORES //descripción de la vlan
#
vlan 2
 description VOZ
#
vlan 5
```

```
 description Centro_Conmutacion
 name CCONMUTA
#
vlan 11
 description Unidad_Ejecutora
 name UNIEJE
#
vlan 12
 description Dep_Sistemas_Conmutacion
 name COMUDAF1
#
vlan 13
 description Dir_Admin_seguridad
 name SEGU
#
vlan 14
 description Cuarto_Control
 name CCTRL
#
vlan 15
 description Dir_Logistica
 name DIRLOGI
#
vlan 16
 description Dep_control
 name DEPCON
#
vlan 17
 description Dir_Personal
name DIRPER1
#
vlan 18
 description Dir_Personal
 name DIRPER2
#
vlan 19
 description Asuntos_Internacionales
 name ASUINT
#
vlan 20
 description Sala_Reuniones
 name SREU
#
vlan 21
 description Cuartel_General
 name CGRAL
#
vlan 22
 description Dep_Ingenieria
```

```
 name DEPING
#
vlan 23
 description Dep_Contratacion_Publica
 name CONPUB
#
vlan 24
 description Dir_Sanidad
 name SANIDAD
#
vlan 25
 description Dep_Evaluacion_Control
 name EVACTRL
#
vlan 26
 description Dir_Telecomunicaciones
 name DIRTEL
#
vlan 27
 description Dir_Sistemas
name DIRSIST1
#
vlan 28
 description Dir_Sistemas
 name DIRSIST2
#
vlan 29
 description Dir_Sistemas
 name DIRSIST3
#
vlan 30
 description Dir_Sistemas
 name ADMIN
#
vlan 31
 description Dir_Administrativa
 name DIRADM1
#
vlan 32
 description Dir_Administrativa
name DIRADM2
#
vlan 33
 description Dep_Juridica
 name JURIDICO
#
vlan 34
 description Jefatura
 name JEFATURA1
```

```
#
vlan 35
 description Jefatura
 name JEFATURA2
#
vlan 36
 description Dir_Intereses_Nacionales
 name INTNAC
#
vlan 37
 description Desarrollo_Institucional
 name DESAINST
#
vlan 38
 description Dir_Operaciones
 name DIROPE
#
vlan 39
 description Cooperacion_Interinstitucional
 name COOPINTER
#
vlan 40
 description Dir_Doctrina
 name DOCTRINA
#
vlan 41
 description Dir_Planes_Ordenes
 name PLANORD
#
vlan 42
 description Federacion_Deportiva
 name FEDDEP
#
vlan 43
 description Dir_Comunic_Social
 name COMSOC
#
vlan 44
 description Direccion_Investigaciones
 name DIRINV
#
vlan 45
 description Wireless
 name WIRELESS
#
interface Vlan-interface1 //interface de la Vlan
 description SERVIDORES //descripción de la interface
 ip address 10.51.10.50 255.255.255.248 // direccionamiento IP asignado a la vlan
```

```
 ip address 10.10.20.1 255.255.255.128 sub // direccionamiento IP asignado a la vlan alterno
#
interface Vlan-interface11
 description UNIEJE
 ip address 10.10.10.225 255.255.255.224
#
interface Vlan-interface12
 description COMU
 ip address 10.10.11.161 255.255.255.240
#
interface Vlan-interface13
 description SEGU
 ip address 10.10.11.177 255.255.255.240
#
interface Vlan-interface14
 description CCTRL
 ip address 10.10.11.97 255.255.255.240
#
interface Vlan-interface15
 description DIRLOGI
 ip address 10.10.9.193 255.255.255.224
#
interface Vlan-interface16
 description DEPCON
 ip address 10.10.10.32 255.255.255.224
#
interface Vlan-interface17
 description DIRPER1
 ip address 10.10.10.1 255.255.255.224
#
interface Vlan-interface18
 description DIRPER2
 ip address 10.10.10.129 255.255.255.224
#
interface Vlan-interface19
 description ASUINT
 ip address 10.10.11.193 255.255.255.240
#
interface Vlan-interface20
 description SREU
 ip address 10.10.9.1 255.255.255.192
#
interface Vlan-interface21
 description CGRAL
 ip address 10.10.12.33 255.255.255.240
#
interface Vlan-interface22
 description DEPING
```

```
 ip address 10.10.11.33 255.255.255.240
#
interface Vlan-interface23
 description CONPUB
 ip address 10.10.11.209 255.255.255.240
#
interface Vlan-interface24
 description SANIDAD
 ip address 10.10.9.225 255.255.255.224
#
interface Vlan-interface25
 description EVACTRL
 ip address 10.10.11.113 255.255.255.240
#
interface Vlan-interface26
 description DIRTEL
 ip address 10.10.9.161 255.255.255.224
#
interface Vlan-interface27
 description DIRSIST1
 ip address 10.10.10.97 255.255.255.224
#
interface Vlan-interface28
 description DIRSIST2
 ip address 10.10.10.65 255.255.255.224
#
interface Vlan-interface29
 description DIRSIST3
 ip address 10.10.11.65 255.255.255.224
#
interface Vlan-interface30
 description ADMIN
 ip address 10.10.12.65 255.255.255.248
#
interface Vlan-interface31
 description DIRADM1
 ip address 10.10.11.49 255.255.255.240
#
interface Vlan-interface32
 description DIRADM2
 ip address 10.10.9.129 255.255.255.224
#
interface Vlan-interface33
 description JURIDICO
 ip address 10.10.11.81 255.255.255.240
#
interface Vlan-interface34
 description JEFATURA1
 ip address 10.10.10.193 255.255.255.224
```

```
#
interface Vlan-interface35
 description JEFATURA2
 ip address 10.10.11.225 255.255.255.240
#
interface Vlan-interface36
 description INTNAC
 ip address 10.10.11.241 255.255.255.240
#
interface Vlan-interface37
 description DESAINST
 ip address 10.10.9.65 255.255.255.192
#
interface Vlan-interface38
 description DIROPE
 ip address 10.10.12.1 255.255.255.240
#
interface Vlan-interface39
 description COOPINTER
 ip address 10.10.11.129 255.255.255.240
#
interface Vlan-interface40
 description DOCTRINA
 ip address 10.10.12.17 255.255.255.240
#
interface Vlan-interface41
 description PLANORD
 ip address 10.10.10.161 255.255.255.224
#
interface Vlan-interface42
 description FEDDEP
 ip address 10.10.11.145 255.255.255.240
#
interface Vlan-interface43
 description COMSOC
 ip address 10.10.12.49 255.255.255.240
#
interface Vlan-interface44
 description DIRINV
 ip address 10.10.11.1 255.255.255.224
#
interface Vlan-interface45
 description WIRELESS
 ip address 10.10.13.1 255.255.255.0
#
interface Aux0/0/0
#
interface M-Ethernet0/0/0
#
```

```
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet1/0/1 //interface del puerto de conexión
 description Enlace 5500G – 1 //descripción del enlace de conexión
 stp edged-port enable //habilitación de Spanning Tree
 broadcast-suppression pps 3000 // tiempo de supresión de tormentas de broadcast
 port access vlan 5  // declaración de puerto tipo acceso en vlan 5
 #
interface GigabitEthernet1/0/2
 description Enlace 5500G – 2
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 5
#
interface GigabitEthernet1/0/3
 description Enlace Bloque1
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 11 to 16
#
interface GigabitEthernet1/0/4
 description Enlace Bloque2
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 13 to 20 32
#
interface GigabitEthernet1/0/5
 description Enlace Bloque3
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 15 20 to 25 31 to 32
#
interface GigabitEthernet1/0/6
 description Enlace Bloque4
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 20 25 26 to 33
#
```

```
interface GigabitEthernet1/0/7
 description Enlace Bloque4-Wireless
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 45
#
interface GigabitEthernet1/0/8
 description Enlace Bloque5
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 20 25 33 to 37
#
interface GigabitEthernet1/0/9
 description Enlace Bloque6
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 20 25 37 to 43
#
interface GigabitEthernet1/0/10
 description Enlace Bloque7
 stp edged-port enable
 broadcast-suppression pps 3000
 port link-type trunk
 port trunk permit vlan 1 44
#
interface GigabitEthernet1/0/11
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet1/0/12
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet1/0/13
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet1/0/14
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet1/0/15
 stp edged-port enable
```

```
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet1/0/16
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet2/0/1
 description Servidor BDD
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/2
 description Servidor Sigef
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/3
 description Servidor Inventarios
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/4
 description Servidor Correo
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/5
 description Servidor DNS Primario
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/6
 description Servidor DNS Secundario
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/7
 description Servidor BI-03
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/8
 description Servidor BI-02
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/9
```

```
 description Servidor Desarrollo
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/10
 description Servidor BI-01
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/11
 description Servidor BI-04
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/12
 description Servidor Backup
 stp edged-port enable
 broadcast-suppression pps 3000
#
interface GigabitEthernet2/0/13
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet2/0/14
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet2/0/15
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface GigabitEthernet2/0/16
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
#
interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 10.51.10.49 preference 60 //ruta de ruteo por defecto
#
ospf 1  //declaración del protocolo de enrutamiento
 area 0.0.0.0 // declaración del ID área ospf
  network 10.51.10.48 0.0.0.7 //declaración de redes
  network 10.10.9.0 0.0.0.255
  network 10.10.10.0 0.0.0.255
```

```
  network 10.10.11.0 0.0.0.255
  network 10.10.12.0 0.0.0.255
  network 10.10.13.0 0.0.0.255
# //habilitación de SNMP
 snmp-agent
 snmp-agent local-engineid 8000002B001AC1EC2B006877
 snmp-agent community read  enmide acl 2900
 snmp-agent sys-info contact ltapia
 snmp-agent sys-info location Piso2
 snmp-agent sys-info version v1 v3
# // habilitación del protocolo SSH
 ssh user admin authentication-type password
 ssh user admin service-type stelnet
# // creación del banner de bienvenida
 header login %<<SW – 7750 -  ACCESO RESTRINGIDO >>%
#
user-interface aux 0 //detalle de la interface aux 0 7
user-interface vty 0 4 //detalle de la interface vty 0 4
 acl 2900 inbound // habilitación de ACL asignada a la interfaz
 authentication-mode scheme  // declaración del método de autenticación
 protocol inbound ssh //habilitación del protocolo ssh
#
return
```

SWITCH 3COM 5500 – BLOQUE1

```
#
 sysname SW-B1 // nombre del equipo
#
 password-control login-attempt 3 exceed lock-time 120 // número máximo de intentos permitidos para logueo
#
 local-server nas-ip 127.0.0.1 key 3com
# // declaración de usuarios
local-user admin //usuario administrador
 password cipher 2ZRSX\:9O'F95K`+NFa@_1!! // password cifrado para usuario administrador
 service-type lan-access // declaración del tipo de acceso a la lan
 service-type ssh telnet terminal
 level 3 //determinación del nivel de acceso
 local-user monitor // usuario monitor
 password simple monitor // password simple para usuario monitor
 service-type ssh telnet terminal // declaración del tipo de acceso a la lan
 level 1 //determinación del nivel de acceso
#
acl number 2800 // declaración de acl básica
 rule 0 deny source 10.10.9.0 0.0.0.255 //creación de regla para negar todo el tráfico
 rule 1 deny source 10.10.10.0 0.0.0.255
 rule 2 deny source 10.10.11.0 0.0.0.255
```

```
 rule 3 deny source 10.10.12.0 0.0.0.255
 rule 4 deny source 10.10.13.0 0.0.0.255
 rule 5 deny source 10.10.20.0 0.0.0.255
 rule 6 permit source 10.10.12.64 0.0.0.7 //creación de regla para permitir el tráfico de la subred
acl number 2900
 rule 0 permit source 10.10.20.51 0
 rule 1 permit source 10.10.12.64 0.0.0.7
 rule 2 deny
#
acl number 3800 // declaración de acl avanzada
 rule 1 permit ip source 10.10.10.224 0.0.0.31 destination 10.10.10.224 0.0.0.31 //creación de reglas para permitir el tráfico entre miembros de la subred
 rule 2 permit ip source 10.10.11.160 0.0.0.15 destination 10.10.11.160 0.0.0.15
 rule 3 permit ip source 10.10.11.176 0.0.0.15 destination 10.10.11.176 0.0.0.15
 rule 4 permit ip source 10.10.11.96 0.0.0.15 destination 10.10.11.96 0.0.0.15
 rule 5 permit ip source 10.10.9.192 0.0.0.31 destination 10.10.9.192 0.0.0.31
 rule 6 permit ip source 10.10.10.32 0.0.0.31 destination 10.10.10.32 0.0.0.31
 rule 7 permit ip source 10.10.10.0 0.0.0.31 destination 10.10.10.0 0.0.0.31
 rule 8 permit ip source 10.10.10.128 0.0.0.31 destination 10.10.10.128 0.0.0.31
 rule 9 permit ip source 10.10.11.192 0.0.0.15 destination 10.10.11.192 0.0.0.15
 rule 10 permit ip source 10.10.9.0 0.0.0.63 destination 10.10.9.0 0.0.0.63
 rule 11 permit ip source 10.10.12.32 0.0.0.15 destination 10.10.12.32 0.0.0.15
 rule 12 permit ip source 10.10.11.32 0.0.0.15 destination 10.10.11.32 0.0.0.15
 rule 13 permit ip source 10.10.11.128 0.0.0.15 destination 10.10.11.128 0.0.0.15
 rule 14 permit ip source 10.10.9.224 0.0.0.31 destination 10.10.9.224 0.0.0.31
 rule 15 permit ip source 10.10.11.112 0.0.0.15 destination 10.10.11.112 0.0.0.15
 rule 16 permit ip source 10.10.9.160 0.0.0.31 destination 10.10.9.160 0.0.0.31
 rule 17 permit ip source 10.10.10.96 0.0.0.31 destination 10.10.10.96 0.0.0.31
 rule 18 permit ip source 10.10.10.64 0.0.0.31 destination 10.10.10.64 0.0.0.31
 rule 19 permit ip source 10.10.11.64 0.0.0.31 destination 10.10.11.64 0.0.0.31
 rule 20 permit ip source 10.10.11.48 0.0.0.15 destination 10.10.11.48 0.0.0.15
 rule 21 permit ip source 10.10.9.128 0.0.0.31 destination 10.10.9.128 0.0.0.31
 rule 22 permit ip source 10.10.11.80 0.0.0.15 destination 10.10.11.80 0.0.0.15
 rule 23 permit ip source 10.10.10.192 0.0.0.31 destination 10.10.10.192 0.0.0.31
 rule 24 permit ip source 10.10.11.124 0.0.0.15 destination 10.10.11.124 0.0.0.15
 rule 25 permit ip source 10.10.11.240 0.0.0.15 destination 10.10.11.240 0.0.0.15
 rule 26 permit ip source 10.10.9.64 0.0.0.63 destination 10.10.9.64 0.0.0.63
 rule 27 permit ip source 10.10.12.0 0.0.0.15 destination 10.10.12.0 0.0.0.15
 rule 28 permit ip source 10.10.11.128 0.0.0.15 destination 10.10.11.128 0.0.0.15
 rule 29 permit ip source 10.10.12.16 0.0.0.15 destination 10.10.12.16 0.0.0.15
 rule 30 permit ip source 10.10.10.160 0.0.0.63 destination 10.10.10.160 0.0.0.63
 rule 31 permit ip source 10.10.11.144 0.0.0.15 destination 10.10.11.144 0.0.0.15
 rule 32 permit ip source 10.10.12.48 0.0.0.15 destination 10.10.12.48 0.0.0.15
 rule 33 permit ip source 10.10.11.0 0.0.0.31 destination 10.10.11.0 0.0.0.31
 rule 34 permit ip source 10.10.13.0 0.0.0.0 destination 10.10.13.0 0.0.0.0

#
vlan 1
```

```
#
vlan 11 // ID de Vlan
 description UNIDAD_EJECUTORA // descripción de la vlan
 name UNIEJE // nombre de la vlan
#
vlan 12
 description DEP_SISTEMAS_COMUNICACIONES
 name COMU
#
vlan 13
 description DIR_ADM_SEGURIDAD
 name SEGU
#
vlan 14
 description CUARTO DE CONTROL
 name CCTRL
#
vlan 15
 description DIR_LOGISTICA
 name DIRLOGI
#
vlan 16
 description DEP_CONTROL
 name DEPCON
#
interface Vlan-interface1 // interface de la Vlan
 description ADMINISTRACION // descripción de la vlan
 ip address 10.10.20.2 255.255.255.128 // direccionamiento IP asignado a la vlan
#
interface Aux1/0/0
#
interface Ethernet1/0/1 //interface del puerto de conexión
 port access vlan 11 // declaración de puerto tipo acceso en vlan 11
 am user-bind mac-addr 001c-cof8-e33c ip-addr 10.10.10.226 // control de acceso
asociado a mac e ip
#
interface Ethernet1/0/2
 port access vlan 11
 am user-bind mac-addr 0011-1110-5fd3 ip-addr 10.10.10.227
#
interface Ethernet1/0/3
 port access vlan 16
 am user-bind mac-addr 0091-4512-b2d3 ip-addr 10.10.10.234
#
interface Ethernet1/0/4
 port access vlan 14
 am user-bind mac-addr 0016-762a-c3c6 ip-addr 10.10.11.98
#
interface Ethernet1/0/5
```

```
 port access vlan 13
 am user-bind mac-addr 0019-2354-285f ip-addr 10.10.11.178
#
interface Ethernet1/0/6
 port access vlan 11
 am user-bind mac-addr 0010-5a5d-bd7c ip-addr 10.10.10.228
#
interface Ethernet1/0/7
 port access vlan 12
 am user-bind mac-addr 0008-a132-d343 ip-addr 10.10.11.162
#
interface Ethernet1/0/8
 port access vlan 12
 am user-bind mac-addr 001c-f0a7-7727 ip-addr 10.10.11.163
#
interface Ethernet1/0/9
 port access vlan 12
 am user-bind mac-addr 0008-a171-bfe0 ip-addr 10.10.11.164
#
interface Ethernet1/0/10
 port access vlan 14
 am user-bind mac-addr 001c-c000-320f ip-addr 10.10.11.99
#
interface Ethernet1/0/11
 port access vlan 14
 am user-bind mac-addr 0019-d1a7-53cb ip-addr 10.10.11.100
#
interface Ethernet1/0/12
 port access vlan 12
am user-bind mac-addr 0018-1113-8baa ip-addr 10.10.11.165
#
interface Ethernet1/0/13
 port access vlan 11
 am user-bind mac-addr 0002-e3e4-18c3 ip-addr 10.10.10.229
#
interface Ethernet1/0/14
 port access vlan 11
 am user-bind mac-addr 0019-d1ff-71a4 ip-addr 10.10.10.232
#
interface Ethernet1/0/15
 port access vlan 15
 am user-bind mac-addr 0007-e990-8a2a ip-addr 10.10.9.194
#
interface Ethernet1/0/16
 port access vlan 16
 am user-bind mac-addr 0008-a134-0fa1 ip-addr 10.10.10.34
#
interface Ethernet1/0/17
 port access vlan 16
```

```
 am user-bind mac-addr 0019-d1f0-16fb ip-addr 10.10.10.35
#
interface Ethernet1/0/18
 port access vlan 14
 am user-bind mac-addr 0002-a5d0-7177 ip-addr 10.10.11.102
#
interface Ethernet1/0/19
 port access vlan 11
 am user-bind mac-addr 0016-7612-a23b ip-addr 10.10.11.233
#
interface Ethernet1/0/20
 port access vlan 16
 am user-bind mac-addr 0016-8f92-6cbf ip-addr 10.10.11.36
#
interface Ethernet1/0/21
 port access vlan 12
 am user-bind mac-addr 0008-020ab-6310 ip-addr 10.10.11.166
#
interface Ethernet1/0/22
 port access vlan 13
am user-bind mac-addr 0019-d196-08be ip-addr 10.10.11.181
#
interface Ethernet1/0/23
 port access vlan 11
 am user-bind mac-addr 001c-c012-be87 ip-addr 10.10.10.230
#
interface Ethernet1/0/24
 port access vlan 11
 am user-bind mac-addr 0016-76ba-cfef ip-addr 10.10.10.231
#
interface GigabitEthernet1/0/25
#
interface GigabitEthernet1/0/26
#
interface GigabitEthernet1/0/27
#
interface GigabitEthernet1/0/28
 stp edged-port enable //habilitación de Spanning Tree
 broadcast-suppression pps 3000 // tiempo de supresión de tormentas de broadcast
 port link-type trunk // asignación de puerto tipo trunk
 port trunk permit vlan 1 11 12 13 14 15 16 // asignación de vlan para el puerto trunk
 packet-filter inbound ip-group 2800 rule 0 //habilitación de regla de filtrado en la entrada de tráfico
 packet-filter inbound ip-group 2800 rule 1
 packet-filter inbound ip-group 2800 rule 2
 packet-filter inbound ip-group 2800 rule 3
 packet-filter inbound ip-group 2800 rule 4
```

```
 packet-filter inbound ip-group 2800 rule 5
 packet-filter inbound ip-group 2800 rule 6
 packet-filter inbound ip-group 3800 rule 1
 packet-filter inbound ip-group 3800 rule 2
 packet-filter inbound ip-group 3800 rule 3
 packet-filter inbound ip-group 3800 rule 4
 packet-filter inbound ip-group 3800 rule 5
 packet-filter inbound ip-group 3800 rule 6

#
 undo xrn-fabric authentication-mode
#
interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.20.1 preference 60 //ruta de ruteo por defecto
# //habilitación de SNMP
 snmp-agent
 snmp-agent local-engineid 8000002B0012A990A5806877
 snmp-agent community read enmide acl 2900
 snmp-agent sys-info contact ltapia
 snmp-agent sys-info location Piso2
 snmp-agent sys-info version v1 v3
# // habilitación del protocolo SSH
 ssh user admin authentication-type password
 ssh user admin service-type stelnet
# // creación del banner de bienvenida
 header login %(( SWITCH BLOQUE1 -- ACCESO RESTRINGIDO ))%
#
user-interface aux 0 7
user-interface vty 0 4
 acl 2900 inbound
 authentication-mode scheme
 protocol inbound ssh
#
return
```

ANEXO 6. SIMULACIÓN DE LA INFRAESTRUCTURA DE RED DEL MINISTERIO DE DEFENSA

La simulación del modelo propuesto para la red de Datos de la Institución fue desarrollada utilizando un simulador del mercado el cual permite demostrar la funcionalidad del modelo en independencia de la tecnología de equipamiento utilizado, cumpliendo los objetivos enfocados en brindar seguridad, disponibilidad, flexibilidad y escalabilidad. El software utilizado para la simulación es Packet Tracer, paquete propietario de Cisco en la versión 5.3.1.

El modelo diseñado está basado en una topología del tipo jerárquica que permite tener una infraestructura de red flexible que se adapte a los cambios de una forma fácil y ágil sin tener que modificar el modelo aplicado, adicionalmente su estructura facilita el aislamiento de fallas dado que se permite aislar segmentos específicos sin dejar de brindar el servicio al resto de la red, además al contar con control en el tráfico intervlan impide que tráfico no deseado se propague por la red.

A continuación se describe el proceso de simulación realizado, con el fin de validar la funcionalidad del modelo en dependencia de los objetivos planteados.

Dentro de la capa de núcleo su objetivo está enfocado a brindar el servicio de conexión con los diferentes entes asociados, además de asegurar la continuidad del servicio; las capas de distribución y acceso están enfocadas a brindar conexión hacia usuario final teniendo en cuenta criterios de segmentación a nivel lógico, además de control el tráfico generado dentro de las diferentes vlan y aplicar seguridad en el acceso hacia el equipamiento activo.

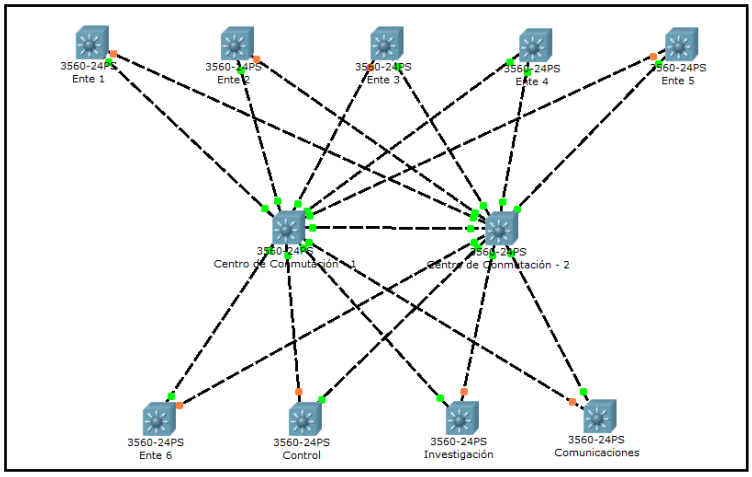


Figura 121. Topología a nivel de acceso y distribución

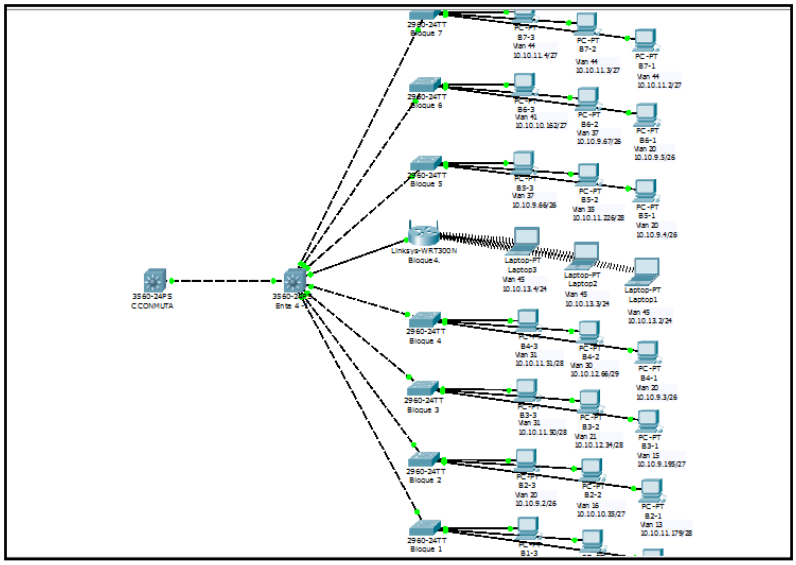


Figura 122. Topología a nivel de capa de acceso y distribución

Ingreso a la administración del equipamiento activo

El ingreso a la configuración del equipamiento activo se encuentra protegido por el uso de contraseñas las mismas que han sido asignadas para los diferentes niveles y el tipo de acceso requerido.

```
hostname Bloque7
!
enable secret 5 $1$mERr$za5EqFDCqdVQ4gbESHSlc/
!
```

Figura 123. Contraseña para modo exec privilegiado

```
line con 0
 password 7 08224D400815001B070103
 login
!
```

Figura 124. Contraseñas para acceso a línea de consola

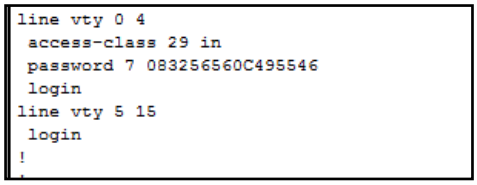


Figura 125. Figura 3. Contraseñas para acceso a terminal vty

Es importante tener en cuenta que las contraseñas deben ser almacenadas de forma cifrada de manera que las mismas no puedan ser filtradas, para ello en la simulación se ha utilizado el servicio de encripción de contraseñas.

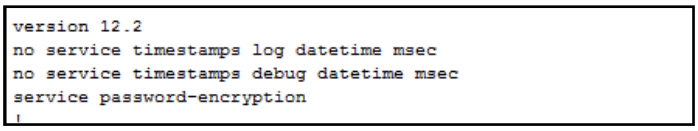


Figura 126. Habilitación servicio de encripción de contraseñas

Teniendo en cuenta que solo personal autorizado debe ingresar hacia la administración del equipamiento activo, solo la vlan de administración podrá contar con acceso remoto para la administración del mismo.

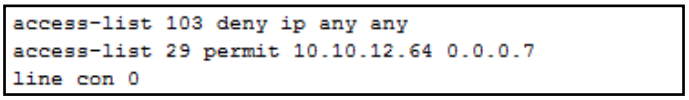


Figura 127. Declaración de ACL para acceso remoto

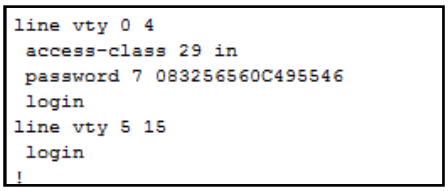


Figura 128. Habilitación de ACL para acceso remoto

Las contraseñas[96] establecidas para acceso a la administración del equipamiento activo utilizando tanto la línea de consola como la administración vía remota se muestran a continuación.

- Contraseña establecida para la línea de consola: **canalelujo**

[96] Estas contraseñas fueron utilizadas netamente dentro del proceso de simulación

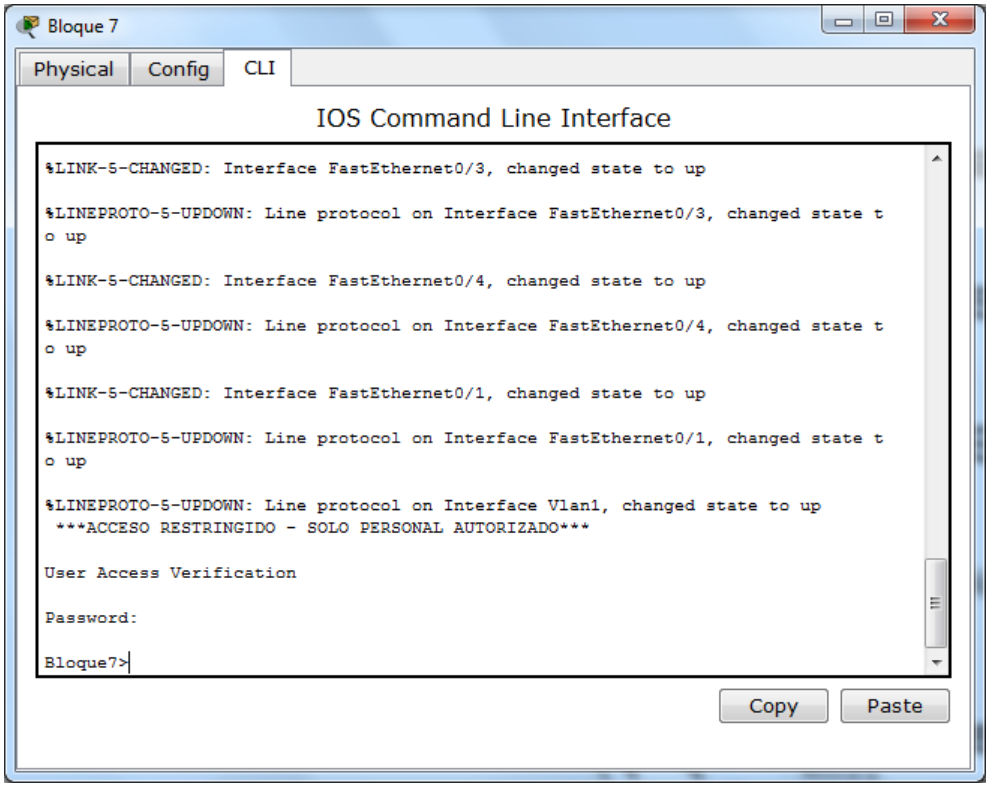


Figura 129. Acceso mediante línea de consola

- Contraseña del modo exec privilegiado: "*nombre del equipo*" ejemplo **bloque7**

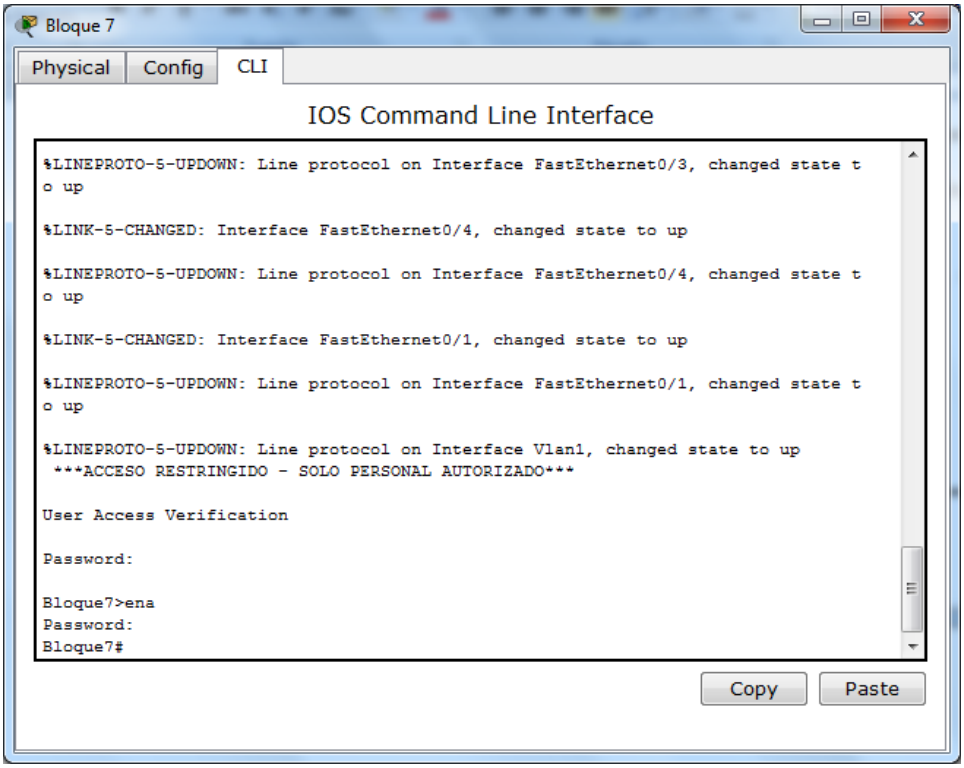


Figura 130. Acceso para el modo exec privilegiado

- Contraseña para acceso remoto tipo telnet: **szxe001**

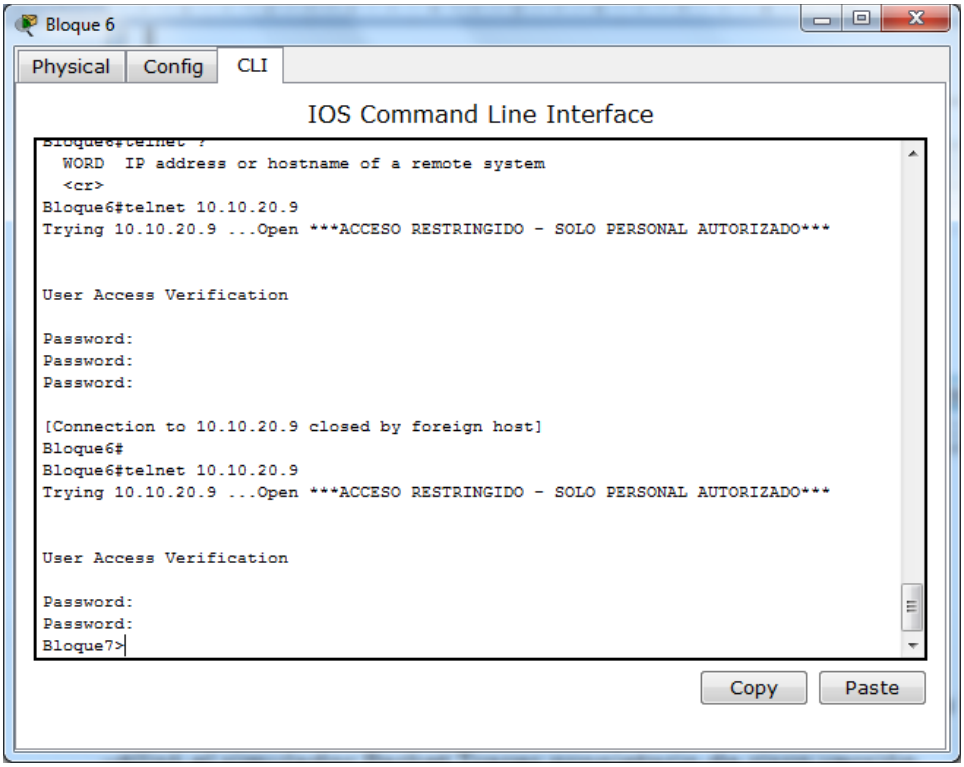


Figura 131. Acceso remoto tipo telnet

Contraseña para acceso remoto tipo ssh: **canalelujo1102**

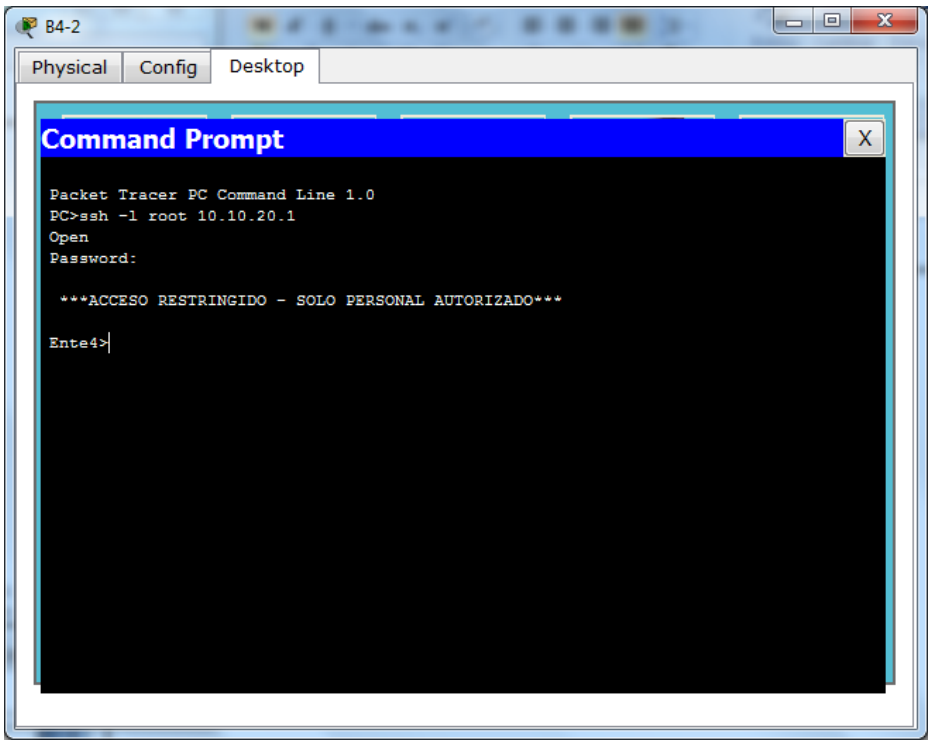


Figura 132. Acceso remoto tipo ssh

Lugo de haber ingresado mediante el terminal virtual el acceso para el modo exec privilegiado se aplica de igual manera que lo indicado: "*nombre del equipo*" ejemplo **ente4**

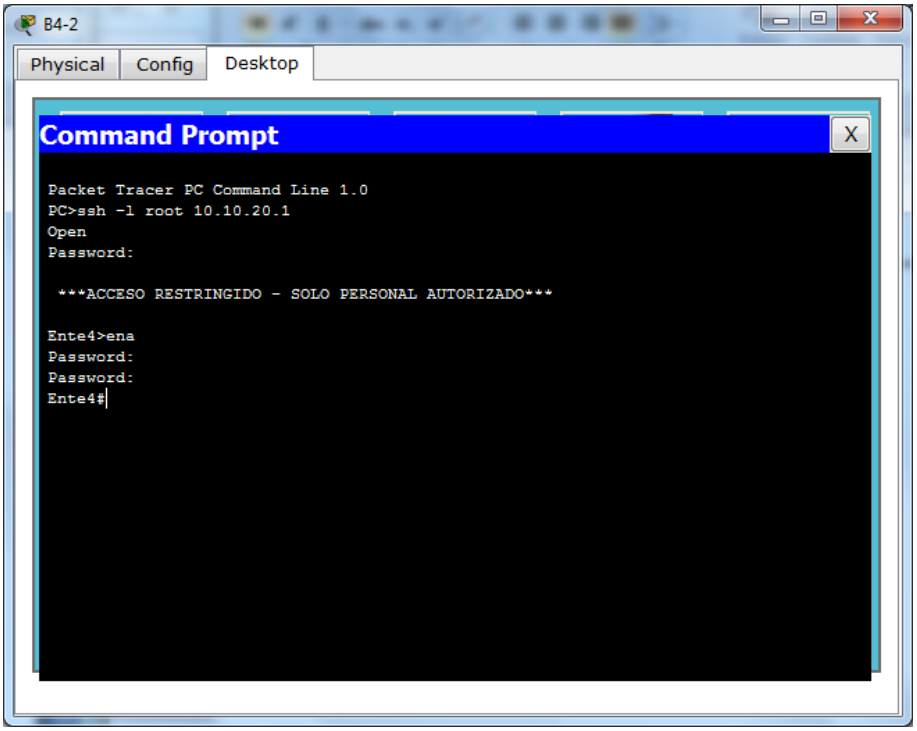


Figura 133. Acceso a terminal de modo exec privilegiado

Es importante que el administrador de red utilice un mecanismo adecuado de implementación de contraseñas, las mismas que deben incluir de preferencia letras mayúsculas, minúsculas, números y caracteres especiales, las mismas que a la par debe ser fáciles de recordar pero no fáciles de adivinar.

Luego de realizar un ingreso exitoso por cualquier medio de conexión se tiene acceso total a la administración del equipamiento, por lo cual es importante tener en cuenta las recomendaciones emitidas debiendo sacarse backup de la configuración antes de realizar cambios en la misma.

Resultados

- El uso de contraseñas para el ingreso a la administración del equipamiento activo protege a los mismos de accesos no autorizados.
- El manejar contraseñas de acceso al equipamiento activo del tipo cifradas protege a los equipos dado que de lograrse un acceso no autorizado a un

nivel de monitoreo, solo se podrá ver la configuración más no las contraseñas utilizadas para el nivel de administración.

- El uso de múltiples contraseñas en base al nivel de configuración a acceder incrementa los controles de seguridad, asegurado el acceso a sólo personal autorizado.
- El ingreso desde solo la subred de administración asegura que solo el personal autorizado ingrese a la administración del equipamiento.

Segmentación de Red

La red de la institución ha sido segmentada en función de diferentes parámetros tomados en cuenta durante el proceso de diseño, como la estructura en base al orgánico funcional, roles y funciones de los usuarios y recursos compartidos; en la simulación se puede observar un pequeño grupos de usuarios asignados en función de la agrupación de las vlans más importantes dentro del modelo; la asignación de usuarios de diferentes vlan permiten validar la funcionalidad de la segmentación aplicada mediante el uso de vlan y la aplicación del direccionamiento IP utilizando VLSM.

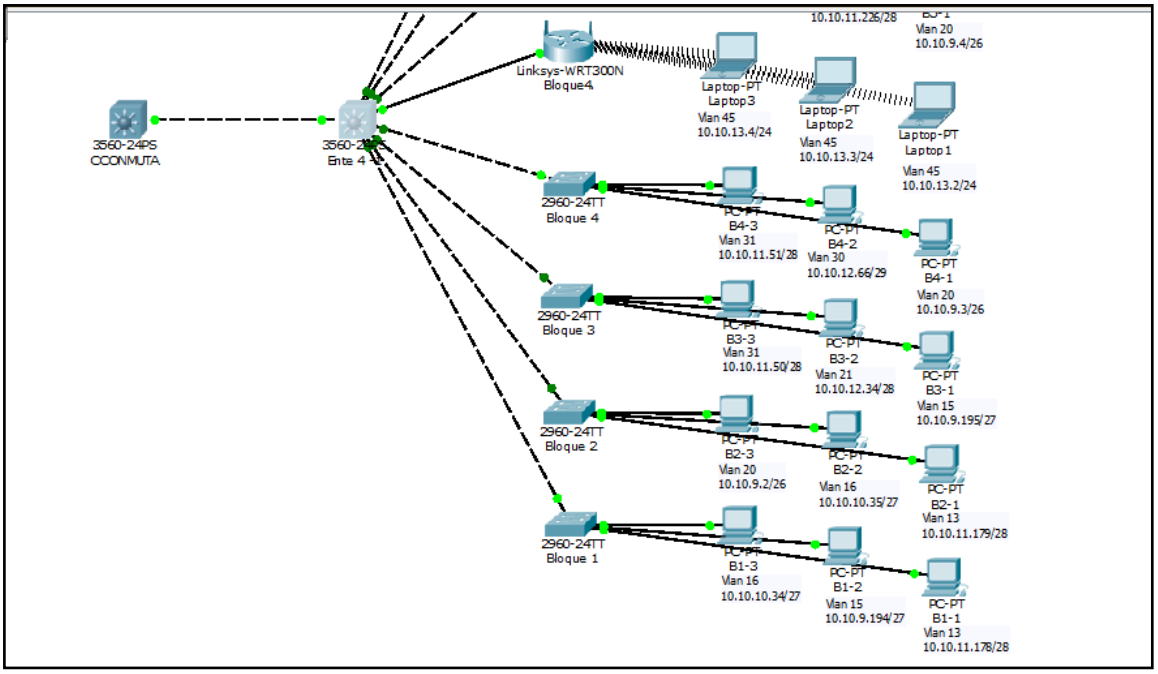


Figura 134. Validación de la segmentación de red

Dentro de la simulación se observa la aplicación de vlan en independencia del bloque asignado de esta manera usuarios con funciones similares pueden compartir una vlan sin importar su ubicación física.

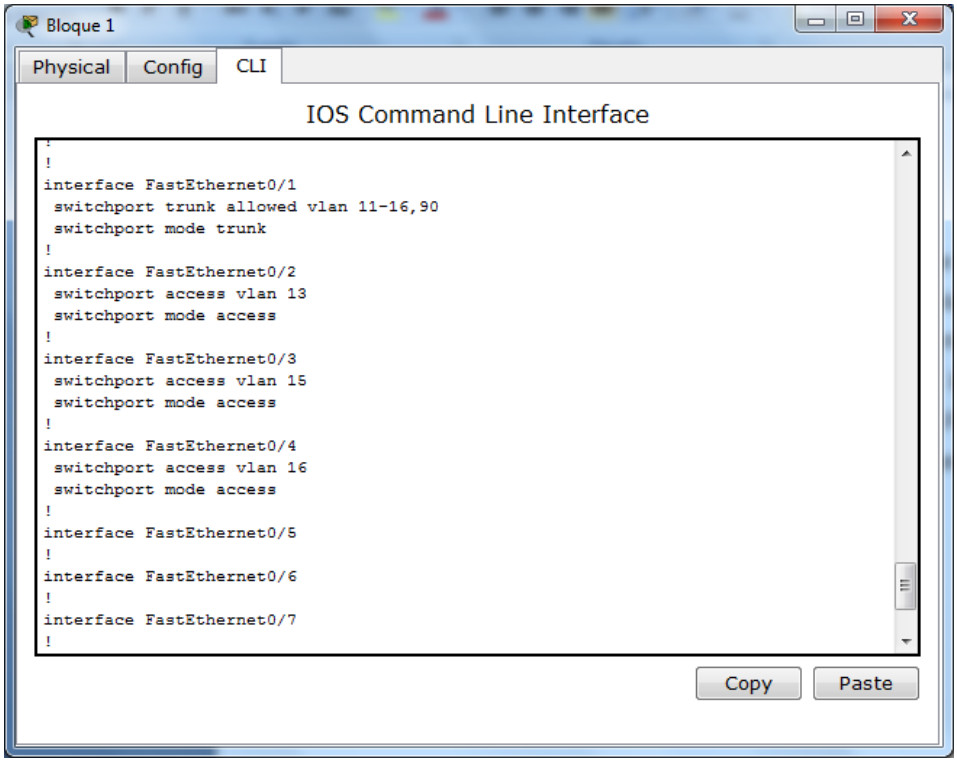


Figura 135. Declaración de puertos de acceso

Así también es importante tener en cuenta que los usuarios necesitan comunicarse solo entre los miembros de la misma vlan por tal motivo el tráfico intervlan está restringido mediante el uso de acl de manera que solo la vlan de administración podrá ver a todas las vlans, para las demás el tráfico está permitido solo entre los miembros de su misma vlan.

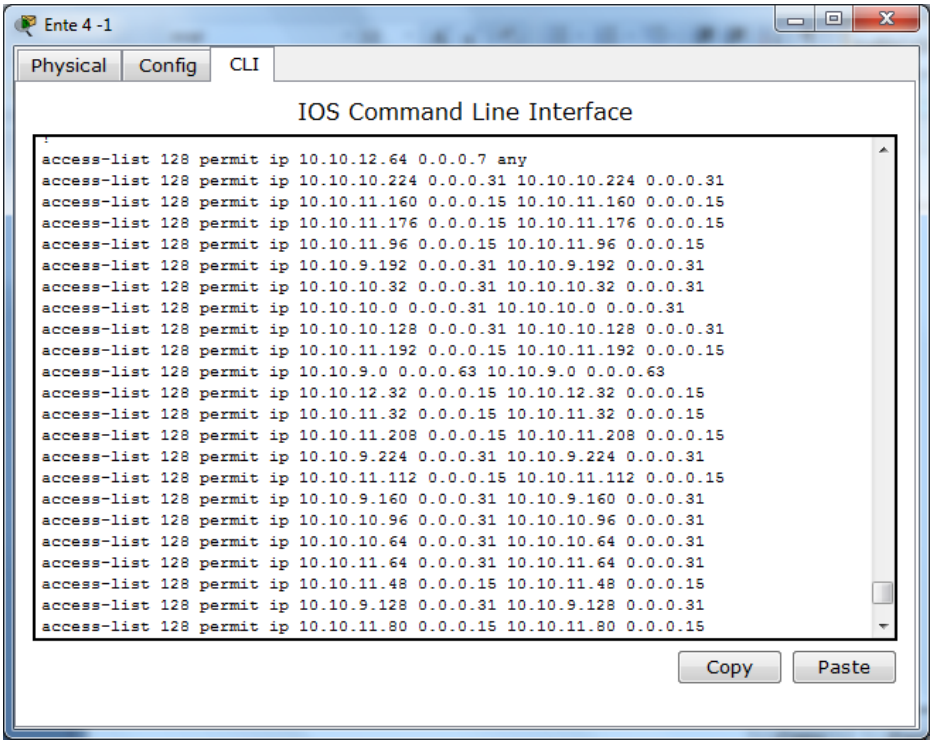


Figura 136. Declaración de ACL para control de tráfico intervlan

La aplicación del direccionamiento IP utilizando vlsm está basada en el estudio de la cantidad de usuarios actuales para cada vlan tomando en cuenta además el crecimiento estimado de la red.

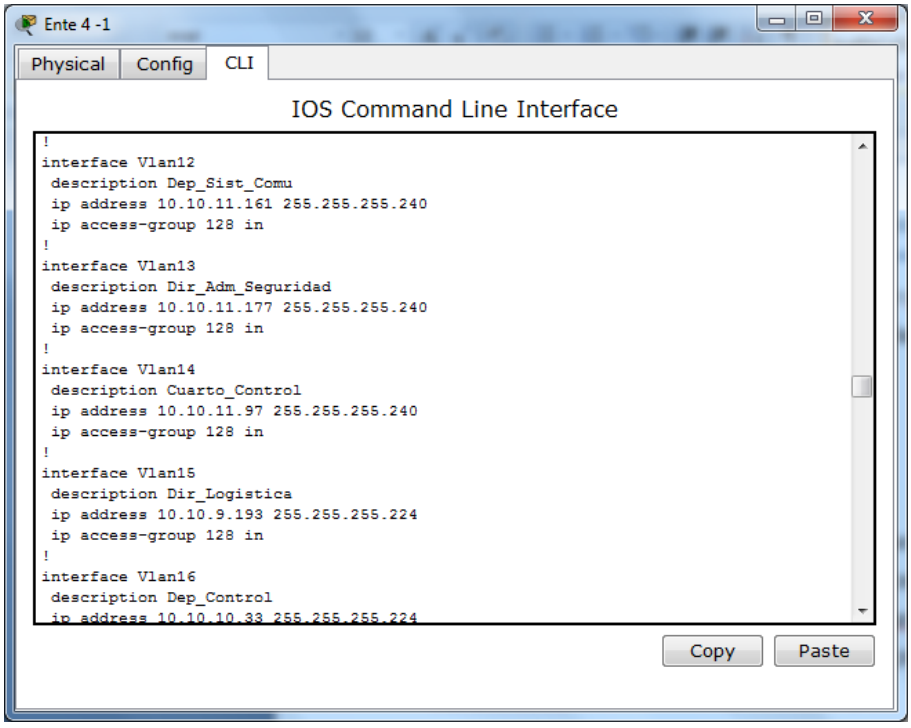


Figura 137. Declaración de vlan

Resultados

El manejo de vlan permite segmentar de manera lógica a la red agrupando a los usuarios en función de sus características, facilitando tareas de administración y brindando seguridad a la red.

El uso de vlan a nivel de acceso limita los dominios de broadcast generados en la red.

Dado que dentro de la aplicación del direccionamiento IP se consideró márgenes de crecimiento a nivel de usuarios la red soporta cambios o adiciones de usuarios a una vlan determinada, así también la aplicación del modelo jerárquico brinda características de flexibilidad al permitirse adaptarse a los cambios sin tener que cambiar su distribución de equipamiento activo.

El uso de listas de control de acceso a más de control el tráfico generado entre los diferentes segmentos de red, protege la red ante el snifereo al cual se encuentra expuesto dado que el tráfico captad será solo de dicho segmento.

Por motivos de administración solo el tráfico generado por la vlan 20 tendrá todos los permisos de acceso hacia el resto de las vlans, para todas las demás el tráfico solo se permite entre los miembros de su propia vlan.

La utilización de VLSM para la asignación del direccionamiento IP evita el desperdicio de direcciones de red.

Asignación de usuarios

En función de la asignación de los usuarios a la vlan se debe configurar el puerto físico de red en el switch del tipo acceso con la vlan especificada; también es importante que en función de las vlans que se utilicen en cada uno de los bloques se defina el paso de las vlans por el puerto de conexión con el equipamiento de la capa distribución (puerto trunk).

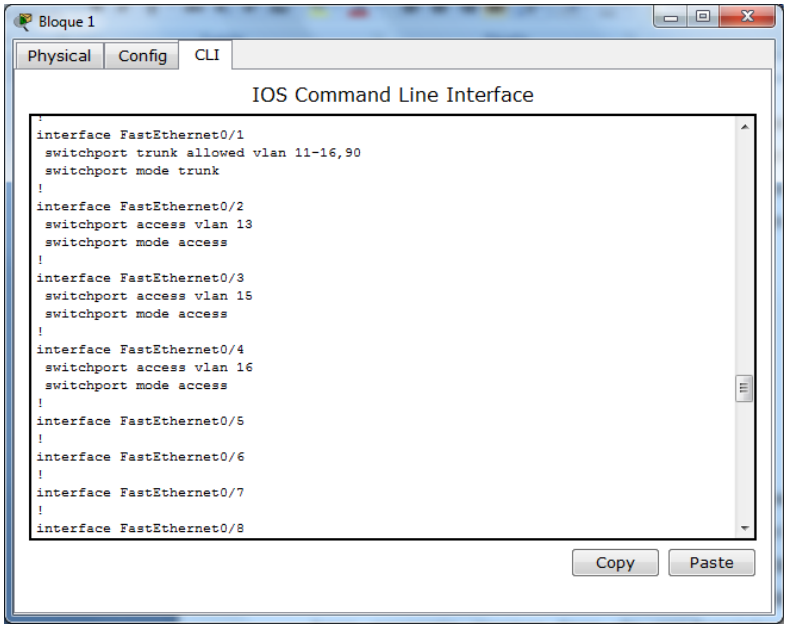


Figura 138. Configuración de puerto tipo acceso y trunk

Resultados

- Con el uso de puertos tipo trunk se permite pasar múltiples vlan por un mismo enlace de manera que un equipo de acceso pueda utilizarlas en función de un modelo dado.
- La configuración de solo las vlan utilizadas en un bloque determinado facilita la administración del equipamiento además de brindar seguridad a la red.
- La asignación de usuarios a una vlan específica, brinda conectividad hacia usuario final.
- El aplicar seguridad para acceso a la red asegura que solo personal autorizado sea el que se encuentra conectado a la red.
- Facilidad de administración, dado que cuando se produce un fallo el personal encargado sabe directamente en donde debe centrar su atención.

Enrutamiento Dinámico

Dado que la infraestructura experimenta varios cambios a nivel de su infraestructura interna de red y como estándar de las Fuerzas Armadas se ha establecido el uso del protocolo OSPF el equipo de distribución debe también entender el mismo protocolo de manera que sea él quien difunda sus redes directamente conectadas.

El área manejada por la institución es el área 0 y las subredes asignadas dentro de la misma están desde la 10.10.9.0 hasta la 10.10.13.0.

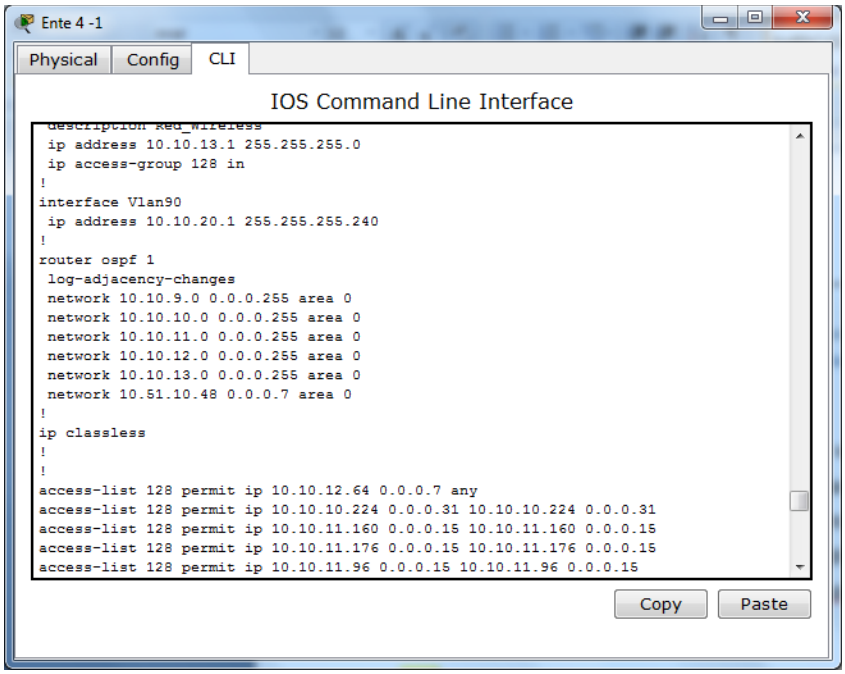


Figura 139. Configuración del protocolo ospf

Resultados

El manejo de un protocolo de enrutamiento dinámico brinda mayor adaptabilidad a la red dado que cualquier cambio solo debe realizarse en la infraestructura en cuestión para las demás el cambio será difundido automáticamente asegurando la comunicación en los dos extremos.

Facilidad de administración al tener que publicar solo las redes directamente conectadas, de esta manera no es necesario conocer a detalle toda la topología de red a la cual se espera conectarse.

Habilitación STP

Teniendo en cuenta que la infraestructura de red debe poseer alta disponibilidad el manejo del protocolo STP asegura una topología libre de bucles, permitiendo que si un enlace físico o equipo de comunicación falle, el tráfico se encamine por otro enlace asegurando su comunicación.

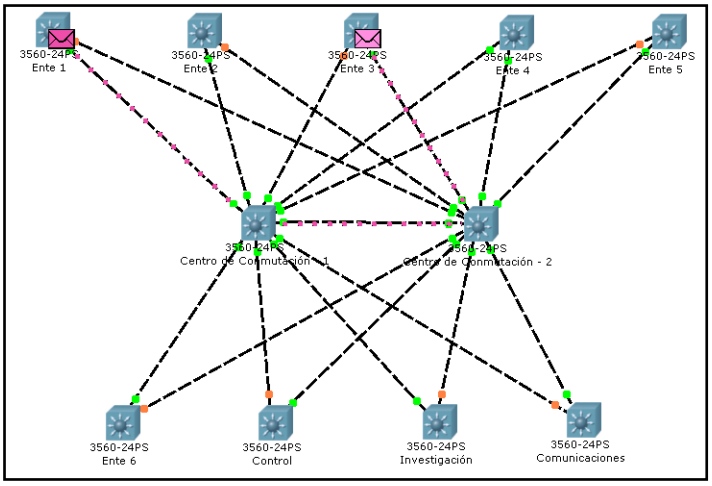


Figura 140. Encaminamiento para entrega de Ente1 a Ente3- caso 1

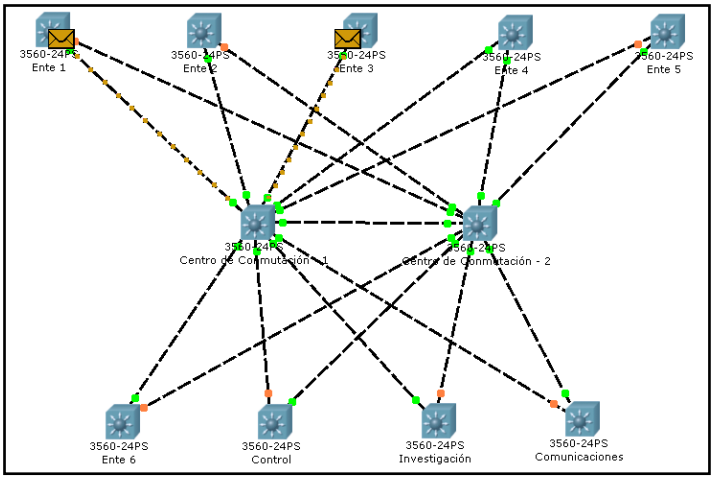


Figura 141. Encaminamiento para entrega de Ente1 a Ente3- caso 2

En las figuras se muestra el caso del envío de un paquete cuando se cuenta con toda la infraestructura activa y uno de los puertos del enlace se encuentra en estado de espera, cuando uno de los enlaces falla toma el control el segundo enlace y se procede a enviar los mismos por la nueva ruta asignada para la entrega del paquete.

Resultados

- Con una topología redundante se asegura la continuidad del servicio y aumenta su tolerancia a fallos.
- El uso de una infraestructura disponible permite que la red sea convergente y pueda brindar nuevos servicios a la red.